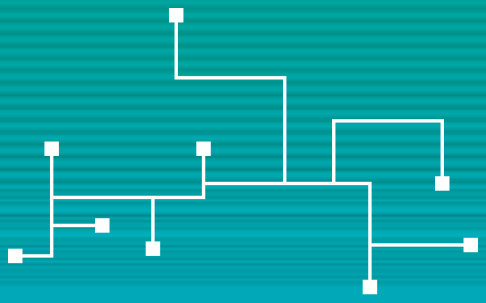

Identidade Dixital

Identidad Digital

XUNTA DE GALICIA

Identidade Dixital - Identidad Digital

Autores: Varios

Edita: Consellería de Cultura, Educación e Ordenación Universitaria

Depósito Legal: C 1937-2017

ÍNDICE

PRESENTACIÓN

Seguindo a "Guía para usuarios: identidade dixital e reputación on line", do Instituto Nacional de Tecnoloxías da Comunicación (INTECO), a identidade dixital pode ser definida como o conxunto de información sobre un individuo ou unha organización (datos persoais, imaxes, rexistros, noticias, comentarios, etc.) exposta en Internet, que conforma unha descrición da dita persoa no plano dixital.

A irrupción na vida cotiá das contornas 2.0, os servizos de mensaxería instantánea e as redes sociais, proporcionan numerosas vantaxes e comodidades. O seu potencial é indiscutiblemente inmenso, pero tamén o son os riscos para a intimidade e a honra das persoas. A formación nas normas básicas de xestión da identidade dixital de todos os membros da comunidade educativa, en calidade de usuarios da comunidade global de Internet, facilitará a creación dun adecuado clima e hábito de uso, e forneceraos de ferramentas axeitadas.

É por isto que a Estratexia Galega de Convivencia 2015-2020 (Educonvives.gal) incluíu no Eixe 3. Apoio aos centros e á comunidade educativa>Obxectivo 3.3 – Establecer protocolos tanto normativos como orientativos que, no marco da autonomía dos centros, favoreza a abordaxe das diferentes situacións de conflito de modo propedéutico, a acción clave "Información e formación sobre aspectos básicos da identidade dixital".

Esta información e formación debe ir dirixida a toda a comunidade educativa. Por suposto ao alumnado, pero tamén ao profesorado e ás familias que son quen exerce o labor de acompañamento na contorna dixital, tan necesario para o axeitado desenvolvemento do alumnado e a adquisición de habilidades, destrezas e competencias de cidadanía dixital activa e responsable.

Paralelamente, no curso 2017-2018 introdúcese por primeira vez a materia de libre configuración autonómica "Identidade Dixital" para primeiro e segundo de ESO, o que supón outro paso máis na educación do alumnado no exercicio das competencias do século XXI.

Nun formato dinámico de preguntas e respostas, tanto en texto como en pílulas de vídeo, faremos un repaso por aqueles conceptos, cuestións e inquedanzas que debemos enfrontar como comunidade educativa. Neste empeño, nesta labor de comunidade, é importante contar con axentes referentes de éxito na xestión da contorna e identidade dixital, como comunidade educativa galega que somos. Por iso a participación de tantas e tan variados persoeiros é un indicador de diversidade, pluralidade e calidade de achegamento da realidade dixital ao día a día nos centros educativos e tamén nos fogares.

Grazas a todas e todos por participar.

Siguiendo la "Guía para usuarios: identidad digital y reputación on line", del Instituto Nacional de Tecnologías de la Comunicación (INTECO), la identidad digital puede ser definida como el conjunto de información sobre un individuo o una organización (datos personales, imágenes, registros, noticias, comentarios, etc.) expuesta en Internet, que conforma una descripción de dicha persona en el plano digital.

La irrupción en la vida cotidiana de los entornos 2.0, los servicios de mensajería instantánea y las redes sociales, proporcionan numerosas ventajas y comodidades. Su potencial es indiscutiblemente inmenso, pero también lo son los riesgos para la intimidad y la honra de las personas. La formación en las normas básicas de gestión de la identidad digital de todos los miembros de la comunidad educativa, en calidad de usuarios de la comunidad global de Internet, facilitará la creación de un adecuado clima y hábito de uso, y les suministrará las herramientas idóneas.

Es por esto que la Estrategia Gallega de Convivencia 2015-2020 (Educonvives.gal) ha incluido en el Eje 3. Apoyo a los centros y a la comunidad educativa>Objetivo 3.3 - Establecer protocolos tanto normativos como orientativos que, en el marco de la autonomía de los centros, favorezca el abordaje de las diferentes situaciones de conflicto de modo propedéutico, la acción clave "Información y formación sobre aspectos básicos de la identidad digital".

Esta información y formación debe ir dirigida a toda la comunidad educativa. Por supuesto al alumnado, pero también al profesorado y a las familias que son quien ejerce la labor de acompañamiento en el entorno digital, tan necesario para el idóneo desarrollo del alumnado y la adquisición de habilidades, destrezas y competencias de ciudadanía digital activa y responsable.

Paralelamente, en el curso 2017-2018 se introduce por primera vez a materia de libre configuración autonómica "Identidad Digital" para primero y segundo de ESO, lo que supone otro paso más en la educación del alumnado en el ejercicio de las competencias del siglo XXI.

En un formato dinámico de preguntas y respuestas, tanto en texto como en píldoras de vídeo, haremos un repaso por aquellos conceptos, cuestiones e inquietudes que debemos enfrentar como comunidad educativa. En este empeño, en esta labor de comunidad, es importante contar con agentes referentes de éxito en la gestión del entorno e identidad digital, como comunidad educativa gallega que somos. Por eso la participación de tantas y tan variadas figuras es un indicador de diversidad, pluralidad y calidad de acercamiento de la realidad digital al día a día en los centros educativos y también en los hogares.

Gracias a todas y todos por participar.

ALBA ALONSO

Doutora en Filoloxía inglesa, Máster en Estudos Ingleses Avanzados, Filóloga e Mestra. A miña tese doutoral foi a faísca que iniciou un apaixonado camiño cara ao emprendemento e que se materializou no proxecto socioeducativo Realkiddys. Autora do conto infantil "Martín es el mejor" e mais a serie de libros de colorear "Coeducando-Coloreando" contra os estereotipos de xénero.

Doctora en Filología inglesa, Máster en Estudios Ingleses Avanzados, Filóloga y Maestra. Mi tesis doctoral fue la chispa que inició un apasionado camino hacia el emprendimiento y que se materializó en el proyecto socioeducativo Realkiddys. Autora del cuento infantil "Martín eres el mejor" y la serie de libros de colorar "Coeducando-Coloreando" contra los estereotipos de género.

Que é o *sexting*?

O *sexting* é o envío de todo tipo de imaxes ou vídeos con algún tipo de contido sexual a través das redes sociais. As mensaxes de texto con este tipo de contido tamén poden ser consideradas como *sexting*.

Os proxenitores poden controlar as contas en redes sociais e o correo electrónico/servizo de mensaxes dos seus fillos e fillas.

Mais que controlar eu aconsellaría supervisar. Para exemplificalo, non é cuestión de non deixarlle o coche, senón de asegurarse que teña o carné de conducir, que respecte ben as normas de tráfico e que sexa consciente da cantidade de perigos que levar un coche poden concorrer. Iso non quita que conducir é una experiencia marabillosa e moi útil para calquera persoa.

Xa que no uso das redes o alumnado ou os nosos fillos e fillas non teñen que sacar carné ningún, é a nosa responsabilidade establecer unha serie de normas moi claras para o uso das redes polos nosos fillos e fillas. Normas en canto ao tempo de utilización, a posibilidade puntual da nosa supervisión, as horas permitidas etc. Tamén podemos facer uso de filtros e programas que bloqueen determinados contidos nos móbiles dos nosos fillos e fillas.

É malo coñecer xente por Internet?

Non creo que sexa malo coñecer xente por Internet. Pero un ou unha adolescente non sempre ten a mesma intuición e atención que unha persoa adulta si debería ter. Tamén deberemos incluír aquí unha serie de normas a respecto destas conexións virtuais. Nada de información

¿Qué es el *sexting*?

El *sexting* es el envío de todo tipo de imágenes o vídeos con algún tipo de contenido sexual a través de las redes sociales. Los mensajes de texto con este tipo de contenido también pueden ser considerados como *sexting*.

Los progenitores pueden controlar las cuentas en redes sociales y el correo electrónico/servicio de mensajería de sus hijos e hijas.

Más que controlar yo aconsejaría supervisar. Para ejemplificarlo, no es cuestión de no dejarle el coche, sino de asegurarse de que tenga el carnet de conducir, que respete bien las normas de tráfico y que sea consciente de la cantidad de peligros que llevar un coche pueden concurrir. Eso que no quita que conducir es una experiencia maravillosa y muy útil para cualquier persona.

Ya que en el uso de las redes nuestro alumnado o hijos e hijas no tienen que sacar carnet alguno, es nuestra responsabilidad establecer una serie de normas muy claras para el uso de las redes por nuestros hijos y hijas. Normas en cuanto al tiempo de utilización, la posibilidad puntual de nuestra supervisión, las horas permitidas etc. También podemos hacer uso de filtros y programas que bloqueen determinados contenidos en los móviles de nuestros hijos e hijas.

¿Es malo conocer gente por Internet?

No creo que sea malo conocer a gente por Internet. Pero un o una adolescente no siempre tiene la misma intuición y

persoal, nada de quedadas físicas e moita información pola nosa parte sobre situacións reais que acontecen con nenos e nenas que si confían en determinados perfís cos que conectan e que ao final acaban por ser pederastas.

Que é a *netiqueta* e cales son as súas regras básicas?

A *netiqueta* refírese ao tipo de comportamento que é axeitado ter no uso das redes sociais. Do mesmo xeito que non imos ao traballo en traxe de baño nin falamos a berros, nas redes sociais deben de cumprirse unha serie de puntos para que todos e todas sexamos respectados e respectadas. Para min, a primeira regra sería: "Non lle digas a ninguén algo polas redes que xamais lle dirías na cara". Isto xa freará moitísimos problemas. Se nos respectamos non usaremos unha linguaxe inadecuada, non seremos desagradables, non interromperemos conversacións con *spam*... Poderiamos incluír moitísimas regras de *netiqueta* pero ao final todo o mundo pode ir aprendendo aos poucos sobre elas, como que o feito de usar maiúsculas significa gritar. Pero o esencial é ese respecto ás opinións dos demais. Podemos debater, engadir, refutar, pero sempre con respecto e tolerancia.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

O meu consello é incluír este mundo nas nosas vidas tamén para poder entendelo e desfrutalo cos nosos fillos e coas nosas fillas. Se non estamos no seu mundo pouco poderemos facer. E eles e elas estarán encantados e encantadas de explicarnos como vai o Facebook, o Twitter ou o Snapchat. Nós podemos ser un marabilloso ou un penoso exemplo para eles e para elas. Se usamos as redes a todas as horas, non lles podemos pedir que só as empreguen un momento. Se interrompemos a nosa comida para contestar un chío, non lles podemos dicir que non teñan o teléfono na mesa. Se cando son pequenos ou pequenas lles damos o móbil ou a tableta para "entreterse" non lla poderemos quitar máis adiante porque "é malo".

As tecnoloxías e as redes teñen moitísimas vantaxes, pero igual que o coche hai que

atención que una persona adulta sí debería tener. También deberemos incluir aquí una serie de normas respeto a estas conexiones virtuales. Nada de información personal, nada de quedadas físicas y mucha información por nuestra parte sobre situaciones reales que le suceden a niños y niñas que sí confían en determinados perfiles con los que conectan y que al final acaban siendo pederastas.

¿Qué es la *netiqueta* y cuáles son sus reglas básicas?

La *netiqueta* se refiere al tipo de comportamiento que es pertinente tener en el uso de las redes sociales. Al igual que no vamos al trabajo en bañador ni hablamos a gritos, en las redes sociales deben cumplirse una serie de puntos para que todos y todas seamos respetados y respetadas. Para mí, la primera regla sería: "No le digas a nadie algo por las redes que jamás le dirías a la cara". Esto ya frenará muchísimos problemas. Si nos respetamos no usaremos un lenguaje inadecuado, no seremos desagradables, no interrumpiremos conversaciones con *spam*... Podríamos incluir muchísimas reglas de *netiqueta* pero al final todo el mundo puede ir aprendiendo poco a poco sobre ellas, como que el hecho de usar mayúsculas significa gritar. Pero lo esencial es ese respeto a las opiniones de los demás. Podemos debatir, añadir, refutar, pero eso sí, siempre con respeto y tolerancia.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Mi consejo es incluir este mundo en nuestras vidas también para poder entenderlo y disfrutarlo con nuestros hijos y con nuestras hijas. Si no estamos en su mundo poco podremos hacer. Y ellos y ellas estarán encantados y encantadas de explicarnos cómo funciona Facebook, Twitter o Snapchat. Nosotros podemos ser un maravilloso o un penoso ejemplo para ellos y para ellas. Si usamos las redes a todas horas, no les podemos pedir que solo las usen un rato. Si interrumpimos nuestra comida para contestar un tweet, no les podemos decir que no tengan el teléfono en la mesa. Si cuando son pequeños o pequeñas les damos el móvil o la tableta para "entretenerse", no se lo podremos quitar más adelante porque "es malo".

saber usalas. De nós depende que eles e mais elas as desfruten dun xeito adecuado.

Las tecnologías y las redes tienen muchas ventajas, pero igual que el coche hay que saber usarlas. De nosotros depende que ellos y ellas las disfruten de manera adecuada.

BELÉN BARRAGÁNS MARTÍNEZ

Doutor Enxeñeiro de Telecomunicación pola Universidade de Vigo. Foi docente da Escola de Enxeñaría de Telecomunicación entre 2000 e 2010. Desde 2010 é Profesora-Secretaria de Centro no Centro Universitario da Defensa na Escola Naval Militar (Marín) onde ademais imparte unha materia relacionada coa programación e os computadores aos futuros Oficiais da Armada.

Doctor Ingeniero de Telecomunicación por la Universidad de Vigo. Fue docente de la Escuela de Ingeniería de Telecomunicación entre 2000 y 2010. Desde 2010 es Profesora-Secretaria de Centro en el Centro Universitario de la Defensa en la Escuela Naval Militar (Marín) donde además imparte una materia relacionada con la programación y los ordenadores a los futuros Oficiales de la Armada.

Cales son os riscos de estafa actuais en Internet e como podemos previlos?

Son múltiples e foron avanzando conforme en Internet apareceron novos servizos. A maioría baséanse, do mesmo xeito que as antigas estafas, en gañar a confianza de usuarias e usuarios inxenuos. Para iso, presentando algo atractivo (gañamos un premio, véndennos un coche ou unha viaxe moi barata) conseguen que realicemos algunha acción (descargar un ficheiro -nos casos menos graves- ou pagar unha cantidade de diñeiro) que non leva aparelladas as consecuencias que esperabamos. Estas accións pódense combater aplicando o sentido común e non crendo en ofertas que, por moi ben que soen, é difícil que sexan reais.

Que son os virus informáticos e como podo defenderme deles?

Os virus informáticos, entendidos como aqueles programas que tiñan como finalidade que os equipos deixasen de funcionar, están a desaparecer mentres que proliferan os ataques baseados en técnicas de enxeñaría social combinados co emprego de software malicioso cuxo principal obxectivo é apoderarse de información ou do propio equipo con distintas finalidades: secuestro de información, creación de *botnets* (para ataques DDoS), etc.

Para minimizar os ataques de software malicioso ou virus informáticos é recomendable ter instalado un antivirus, ter actualizado o sistema operativo e empregar unha gran dose de sentido común para non ser vítimas de enxeñaría social: non pulsar en ligazóns remitidas por cor-

¿Cuáles son los riesgos de estafa actuales en Internet y cómo podemos prevenirlos?

Son múltiples y han ido avanzando a medida que en Internet han ido apareciendo nuevos servicios. La mayoría se basan, al igual que los antiguos timos, en ganarse la confianza de usuarias y usuarios ingenuos. Para ello, presentando algo atractivo (hemos ganado un premio, nos venden un coche o un viaje muy barato) consiguen que realicemos alguna acción (descargar un fichero -en los casos menos graves- o pagar una cantidad de dinero) que no lleva aparejadas las consecuencias que esperábamos. Estas acciones se pueden combatir aplicando el sentido común y no creyéndonos ofertas que, por muy bien que suenen, es difícil que sean reales.

¿Qué son los virus informáticos y cómo puedo defenderme de ellos?

Los virus informáticos, entendidos como aquellos programas que tenían como finalidad que los equipos dejasen de funcionar, están desapareciendo mientras que proliferan los ataques basados en técnicas de ingeniería social combinados con el empleo de software malicioso cuyo principal objetivo es apoderarse de información o del propio equipo con distintas finalidades: secuestro de información, creación de *botnets* (para ataques DDoS) etc.

Para minimizar los ataques de software malicioso o virus informáticos es recomendable tener instalado un antivirus, tener actualizado el sistema operativo y emplear una gran dosis de sentido común para no ser víctimas de ingeniería social: no pulsar en enlaces remitidos por correo

reo electrónico nin abrir ficheiros adxuntos (aínda cando o correo nos pareza que ten unha procedencia segura), non darlle a ninguén as nosas claves nin datos de cartóns de crédito por correo (o noso banco non nos vai pedir datos deste tipo por correo electrónico), etc.

Como é un contrasinal seguro? Que trucos podo utilizar para xerar e manter contrasinais seguros?

Un contrasinal seguro é aquel que é suficientemente complexo. Para que non sexa fácil de adiviñar, non debe estar baseado en palabras do dicionario nin conter datas persoais. Deberá ter unha lonxitude mínima de oito caracteres e incluír maiúsculas, minúsculas, números e algúns caracteres tipo %&$.

Un truco para xerar contrasinais robustos e non esquecernos deles pode consistir en empregar unha frase que lembremos ben (a letra dunha canción que nos guste, por exemplo) e quedar coas iniciais de cada palabra. De transformarmos algunha desas letras nun número, por exemplo, un <e> nun 3 ou un <o> nun 0; pasarmos algunha letra a maiúscula e engadirmos algúns caracteres dos antes mencionados, poderiamos ter xa un bo contrasinal. De non querermos usar a mesma en todos os sitios web que empregamos (o que é moi recomendable), podemos engadir ao contrasinal anterior, que usaremos como base, as terminacións -gm (para Gmail), -fb (para Facebook) etc.

Que é a suplantación de identidade en Internet e que consecuencias ten?

A través da suplantación de identidade, outras persoas poden facerse pasar por nós na Rede, despois de conseguir o noso inicio de sesión e contrasinal nunha determinada rede social, por exemplo, e realizar accións no noso nome, desde publicar contido ou escribir comentarios etc. As consecuencias serán máis ou menos graves en función das accións realizadas. Isto é especialmente grave para as empresas, onde unha suplantación de identidade pode facer perder a confianza da clientela. Así mesmo, podemos sufrir ataques en que quen ataque suplante a identidade do noso banco, por exemplo, solicitándonos información da nosa conta bancaria ou dos nosos cartóns de crédito.

electrónico ni abrir ficheros adjuntos (aun cuando el correo nos parezca que tiene una procedencia segura), no dar nuestras claves ni datos de tarjetas de crédito por correo a nadie (nuestro banco no nos pedirá datos de este tipo por correo electrónico) etc.

¿Cómo es una contraseña segura? ¿Qué trucos puedo utilizar para generar y mantener contraseñas seguras?

Una contraseña segura es aquella que es lo suficientemente compleja. Para que no sea fácil de adivinar, no debe estar basada en palabras del diccionario, ni contener fechas personales. Deberá tener una longitud mínima de ocho caracteres e incluir mayúsculas, minúsculas, números y algún carácter tipo %&$.

Un truco para generar contraseñas robustas y no olvidarnos de ellas puede consistir en emplear una frase que recordemos bien (la letra de una canción que nos guste, por ejemplo) y quedarnos con las iniciales de cada palabra. Transformando alguna de esas letras en un número, por ejemplo, una <e> en un 3 o una <o> en un 0, pasando alguna letra a mayúsculas y añadiendo algún carácter de los antes mencionados podríamos tener ya una buena contraseña. Si no queremos usar la misma en todos los sitios web que empleamos (lo que es muy recomendable), podemos añadir a la contraseña anterior, que usaremos como base, las terminaciones -gm (para Gmail), -fb (para Facebook) etc.

¿Qué es la suplantación de identidad en Internet y qué consecuencias tiene?

A través de la suplantación de identidad, otras personas pueden hacerse pasar por nosotros en la Red, tras haber conseguido nuestro login y contraseña en una determinada red social, por ejemplo, y realizar acciones en nuestro nombre, desde publicar contenido o escribir comentarios etc. Las consecuencias serán más o menos graves en función de las acciones realizadas. Esto es especialmente grave para las empresas, donde una suplantación de identidad puede hacer perder la confianza de su clientela. Asimismo, podemos sufrir ataques en los que quien ataque suplante la identidad de nuestro

Que son as redes P2P e como funcionan? Todo o que circula nelas é libre. É gratuíto?

As redes P2P son redes descentralizadas usadas fundamentalmente para intercambio de arquivos. Funcionan de maneira distribuída, no sentido de que non existen servidores e clientes, senón que un mesmo nodo da Rede pode comportarse como ambos os dous e estar a recibir ficheiros e a compartir outros. Dentro das redes P2P pódense atopar todo tipo de arquivos, desde ficheiros libres e gratuítos, a aqueles que teñen propiedade intelectual, e ás veces mesmo se utilizan para compartir material de pornografía infantil.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

A identidade dixital constrúese a partir de todos os documentos, fotos, etc. relacionados coa nosa persoa en Internet. Debemos ser especialmente coidadosos e coidadosas coa información que publicamos porque, como se adoita dicir, Internet non esquece e, unha vez que os ficheiros abandonan o noso computador, podemos perder o control desa información, en caso de querer eliminala. Cada vez que publicamos algo deberiamos pararnos a pensar dous minutos no seguinte: dentro de trinta anos pódeme importar que alguén vexa esta información? Os meus futuros xefes ou xefas? A miña futura parella? Se cadra con esta pequena autorreflexión non publicariamos tan a treo.

banco, por ejemplo, solicitándonos información de nuestra cuenta bancaria o de nuestras tarjetas de crédito.

¿Qué son las redes P2P y cómo funcionan? ¿Todo lo que circula en ellas es libre? ¿Es gratuito?

Las redes P2P son redes descentralizadas usadas fundamentalmente para intercambio de archivos. Funcionan de manera distribuida, en el sentido de que no existen servidores y clientes, sino que un mismo nodo de la Red puede comportarse como ambos y estar recibiendo ficheros y compartiendo otros. Dentro de las redes P2P se pueden encontrar todo tipo de archivos, desde ficheros libres y gratuitos, a aquellos que tienen propiedad intelectual, e incluso a veces se utilizan para compartir material de pornografía infantil.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

La identidad digital se construye a partir de todos los documentos, fotos etc. relacionados con nuestra persona en Internet. Debemos ser especialmente cuidadosos y cuidadosas con la información que publicamos porque, como se suele decir, Internet no olvida y, una vez que los ficheros abandonan nuestro ordenador, podemos perder el control de esa información, en caso de querer eliminarla. Cada vez que publicamos algo deberíamos pararnos a pensar dos minutos lo siguiente: dentro de treinta años, ¿me puede importar que alguien vea esta información? ¿Mis futuros jefes o jefas? ¿Mi futura pareja? A lo mejor con esta pequeña autorreflexión, no publicaríamos tan a la ligera.

Mª LUZ CASTRO PENA

Enxeñeira Superior en Informática pola Universidade da Coruña.

Socia fundadora de **imaxin**|software e directora da súa área de multimedia.

Profesora interina na Facultade de Ciencias da Comunicación da UDC.

Vogal do Comité de Dirección do Clúster TIC.

I Premio Ada Byron do Colexio Profesional de Enxeñería Informática de Galicia (CPEIG).

Ingeniera Superior en Informática por la Universidad de A Coruña.

Socia fundadora de **imaxin**|software y directora de su área de multimedia.

Profesora interina en la Facultad de Ciencias da Comunicación de la UDC.

Vocal del Comité de Dirección del Clúster TIC.

I Premio Ada Byron del Colegio profesional de Ingeniería Informática de Galicia (CPEIG).

As cousas que subimos ás redes sociais como Facebook ou Twitter son privadas, porque só as poden ver as persoas que designamos.

Temos que ter moito coidado coas cousas que subimos ás redes sociais, porque non é só que non sexan privadas, senón que moitas veces deixan de ser nosas, xa que sen sabelo cedemos os nosos dereitos sobre elas.

As condicións de servizo de Facebook (esas que normalmente non lemos) indican:

"outórgasnos unha licenza non exclusiva, transferible, con posibilidade de ser sub-rogada, libre de regalías e aplicable globalmente para utilizar calquera contido de IP que publiques en Facebook ou en conexión con Facebook (licenza de PI). Esta licenza de PI finaliza cando eliminas o teu contido de PI ou a túa conta, a menos que o contido fose compartido con terceiros e estes non o eliminaran".

É dicir, Facebook outórgase unha licenza de uso dos nosos contidos (fotografías, vídeos, etc.) para facer con eles practicamente o que queira.

En canto á privacidade, tampouco é real, porque incluso nas redes sociais con políticas de privacidade nas publicacións, ninguén nos pode asegurar que alguén non teña feito unha captura de pantalla do noso contido, e que poda ser posteriormente redistribuído.

Las cosas que subimos a las redes sociales como Facebook o Twitter son privadas porque solo las pueden ver las personas que designamos.

Tenemos que tener mucho cuidado con las cosas que subimos a las redes sociales, porque no es solo que no sean privadas, sino que muchas veces dejan de ser nuestras, ya que sin saberlo cedemos nuestros derechos sobre ellas.

Las condiciones de servicio de Facebook (esas que normalmente no leemos) indican:

"nos otorgas una licencia no exclusiva, transferible, con posibilidad de ser subrogada, libre de regalías y aplicable globalmente para utilizar cualquier contenido de IP que publiques en Facebook o en conexión con Facebook (licencia de PI). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta, a menos que el contenido fuese compartido con terceros y estos no lo hayan eliminado"

Es decir, Facebook se otorga una licencia de uso de nuestros contenidos (fotografías, vídeos etc.) para hacer con ellos prácticamente lo que quiera.

En cuanto a la privacidad, tampoco es real, porque incluso en las redes sociales con políticas de privacidad en las publicaciones, nadie nos puede asegurar que alguien no haya hecho una captura de pantalla de nuestro contenido, y que pueda ser posteriormente redistribuido.

Un/Unha menor non pode mercar nada por Internet e, de o facer, a empresa está obrigada a devolverlle o diñeiro.

Para comprar por Internet é necesario ter capacidade de contratar. A teoría xeral de contratos di que os menores de idade non emancipados non poden contratar por non poder prestar validamente o seu consentimento. Dado que o consentimento é un elemento esencial do contrato, os contratos nos que unha parte sexa un menor de 18 anos serían anulables (que non nulos), o que significa que os pais (ou titores), ou mesmo o menor cando alcance a maioría de idade, terían a posibilidade durante catro anos de exercitar unha acción para deixar sen efecto o contrato. Pero, se non se exercita, o contrato é válido.

Por tanto, as situacións nas que un contrato celebrado por un menor de idade é plenamente eficaz serían dúas:

a. Aqueles contratos que son habituais de acordo cos usos sociais (pola súa contía ou clase de negocio) en relación coa idade do menor e a súa madurez para comprendelo (por exemplo a compra de xeados, libros ou videoxogos).

b. Aqueles contratos fóra dos casos anteriores pero realizados coa colaboración e coñecemento dos pais, o que loxicamente debería demostrarse.

No resto de supostos, o contrato sería anulable.

O problema nestes casos no ámbito de Internet é que o vendedor ou fornecedor dun servizo non pode comprobar se quen está do outro lado é maior ou menor de idade, ou se ten xuízo ou coñecemento suficiente para poder contratar, a pesar de que nas súas condicións contractuais esixa esa capacidade, o que o pode deixar nunha situación insegura. O vendedor debe tomar medidas para verificar a idade dentro do razoable e asumir os posibles problemas que se xeren por iso, mais tamén non hai que descartar que o propio menor pode enganar á outra parte, mentir sobre a súa idade ou identidade, ou utilizar datos de conta ou cartóns dos seus pais, así que nestes casos, aínda que se anulase o contrato, non é descartable que a parte vendedora poida reclamar danos e prexuízos aos pais, que ao final son responsables dos actos dos seus fillos e filas. Como por exemplo,

Un/a menor no puede comprar nada por Internet y, si lo hace, la empresa está obligada a devolverle el dinero.

Para comprar por Internet es necesario tener capacidad de contratar. La teoría general de contratos dice que los menores de edad no emancipados no pueden contratar por no poder prestar válidamente su consentimiento. Dado que el consentimiento es un elemento esencial del contrato, los contratos en los que una parte sea un menor de 18 años serían anulables (que no nulos), lo que significa que los padres (o tutores), o incluso el menor cuando alcance la mayoría de edad, tendrían la posibilidad durante cuatro años de ejercitar una acción para dejar sin efecto el contrato. Pero, si no se ejercita, el contrato es válido.

Por tanto, las situaciones en las que un contrato celebrado por un menor de edad es plenamente eficaz serían dos:

a. Aquellos contratos que son habituales de acuerdo con los usos sociales (por su cuantía o clase de negocio) en relación con la edad del menor y su madurez para comprenderlo (por ejemplo la compra de helados, libros o videojuegos).

b. Aquellos contratos fuera de los casos anteriores pero realizados con la colaboración y conocimiento de los padres, lo que lógicamente debería demostrarse.

En el resto de supuestos, el contrato sería anulable.

El problema en estos casos en el ámbito de Internet es que el vendedor o prestador de un servicio no puede comprobar si quien está del otro lado es mayor o menor de edad, o si tiene juicio o conocimiento suficiente para poder contratar, a pesar de que en sus condiciones contractuales exija esa capacidad, lo que le puede dejar en una situación insegura. El vendedor debe tomar medidas para verificar la edad dentro de lo razonable y asumir los posibles problemas que se generen por eso, pero también no hay que descartar que el propio menor puede engañar a la otra parte, mentir sobre su edad o identidad, o utilizar datos de cuenta o tarjetas de crédito de sus padres, así que en estos casos, aunque se anulara el contrato, no es descartable que la parte vendedora pueda reclamar daños y perjuicios a los padres, que al final son responsables de

se deixan que o menor xogue co smatphone ou a tablet cos datos de conta e pago ao seu alcance.

Que é un/unha *prosumidor/a*? Por que hai que aprender a xestionar a nosa actuación como *prosumidores/as*?

A palabra prosumidor provén dun acrónimo formado pola fusión das palabras en inglés produtor e consumidor (producer + consumer = prosumer).

Trátase dun termo utilizado en ámbitos moi diferentes, desde a agricultura á informática, e aplícase a aqueles usuarios que ao mesmo tempo que son consumidores, son á súa vez produtores de contidos. Un prosumidor en teoría non ten fins lucrativos, só participa nun mundo dixital de intercambio de información (por exemplo o caso da Wikipedia, cuxos contidos son elaborados e editados polos propios usuarios sen unha remuneración a cambio).

A palabra "prosumidor" describe perfectamente a millóns de participantes na revolución da Web 2.0, xa que son cada vez máis as persoas involucradas que soben información á rede e á súa vez son consumidores da mesma.

Grazas aos avances da tecnoloxía, todos podemos ser produtores de contidos. Se antes a liberdade de prensa unicamente afectaba a quen tiña unha, agora todos podemos escribir, gravar ou filmar o que queiramos e polo a disposición dunha audiencia. Pero ademais, non esquecemos a nosa faceta de consumidores: mantemos relacións con infinidade de empresas cuxos produtos e servizos usamos habitualmente.

Desde o punto de vista das empresas, un prosumidor é calquera persoa coa capacidade de publicar as súas opinións sobre ela, polo tanto, calquera persoa.

Como se respectan os dereitos de propiedade intelectual en Internet?

Toda obra está sometida aos dereitos de autor, aínda que non exista mención que o indique expresamente, e a lexislación sobre dereitos de autor é moi variable dun país a outro.

As infraccións dos dereitos de autor céntranse especialmente na reprodución parcial ou total dunha obra, a súa modi-

los actos de sus hijos e hijas. Como, por ejemplo, si dejan que el menor juegue con el smatphone o la tableta con los datos de cuenta y pago a su alcance.

¿Qué es un/a *prosumidor/a*? ¿Por qué hay que aprender a gestionar nuestra actuación como *prosumidores/as*?

La palabra prosumidor proviene de un acrónimo formado por la fusión de las palabras en inglés productor y consumidor (producer + consumer = prosumer).

Se trata de un término utilizado en ámbitos muy diferentes, desde la agricultura a la informática, y se aplica a aquellos usuarios que al mismo tiempo que son consumidores, son también productores de contenidos. Un prosumidor en teoría no tiene fines lucrativos, solo participa en un mundo digital de intercambio de información (por ejemplo, el caso de la Wikipedia, cuyos contenidos son elaborados y editados por los propios usuarios sin una remuneración a cambio).

La palabra "prosumidor" describe perfectamente a millones de participantes en la revolución de la Web 2.0, ya que son cada vez más las personas involucradas que suben información a la red y a su vez son consumidoras de la misma.

Gracias a los avances de la tecnología, todos podemos ser productores de contenidos. Si antes la libertad de prensa únicamente afectaba a quien tenía una, ahora todos podemos escribir, grabar o filmar lo que queramos y ponerlo a disposición de una audiencia. Pero, además, no olvidemos nuestra faceta de consumidores: mantenemos relaciones con infinidad de empresas cuyos productos y servicios usamos habitualmente.

Desde el punto de vista de las empresas, un prosumidor es cualquier persona con la capacidad de publicar sus opiniones sobre ella, por lo tanto, cualquier persona.

¿Cómo se respetan los derechos de propiedad intelectual en Internet?

Toda obra está sometida a los derechos de autor, aunque no exista mención que lo indique expresamente, y la legislación sobre derechos de autor es muy variable de un país a otro.

Las infracciones de los derechos de autor se centran especialmente en la reproduc-

ficación ou difusión non autorizada, e a súa utilización a título comercial ou non comercial.

Estas limitacións non afectan a utilización dunha obra nun marco privado. Salvo mención contraria (autorización expresa do autor, licenzas ou obras de dominio público), o conxunto das obras seguintes están sometidas ao dereito de autor na Web:

- As imaxes, os vídeos (películas e clips), os audios e as obras musicais.
- Os traballos e obras literarias en: blogs e sitios web, libros, banda deseñada, boletíns de noticias, revistas, memorandos, xornais, manuais e folletos (papel ou formato dixital: arquivos PDF).
- Os programas informáticos.
- As creacións gráficas, mapas xeográficos e infografías.
- As presentacións multimedia.

Como os contidos mencionados anteriormente, as capturas de pantalla dunha imaxe, dun vídeo ou dunha páxina web están sometidos ao dereito de autor e a súa utilización debe teoricamente ser obxecto dunha autorización previa.

Por exemplo, Youtube avisa:

"verifique que todos os compoñentes do seu vídeo son da súa propia creación, incluído a parte de audio. Se vostede utiliza por exemplo unha pista de audio cuxos dereitos de autor son dunha casa de discos que non deu a autorización para usala, o seu vídeo pode atentar contra os dereitos de autor de terceiros e pode ser suprimido."

E a páxina de copyright de Facebook, contén información sobre os dereitos de propiedade intelectual relativos ao contido publicado en Facebook:

"Facebook respecta os dereitos de propiedade intelectual dos autores e comprométese en axudar a protexer os seus dereitos. A nosa Declaración de dereitos e responsabilidades impide aos usuarios publicar contido que infrinxa os dereitos de propiedade intelectual doutro usuario ou autor. Cando recibimos unha declaración válida de violación dos dereitos de propiedade intelectual, suprimimos ou prohibimos o acceso aos materiais en cuestión. Tamén suprimimos as contas dos usuarios reincidentes".

A organización Creative Commons ofre-

ción parcial o total de una obra, su modificación o difusión no autorizada, y su utilización a título comercial o no comercial.

Estas limitaciones no afectan la utilización de una obra en un marco personal. Salvo mención contraria (autorización expresa del autor, licencias u obras de dominio público), el conjunto de las obras siguientes están sometidas al derecho de autor en la Web:

- Las imágenes, los vídeos (películas y clips), los audios y las obras musicales.
- Los trabajos y obras literarias en: blogs y sitios web, libros, cómic, boletines de noticias, revistas, memorándums, periódicos, manuales y folletos (papel o formato digital: archivos PDF).
- Los programas informáticos.
- Las creaciones gráficas, mapas geográficos e infografías.
- Las presentaciones multimedia.

Como los contenidos mencionados anteriormente, las capturas de pantalla de una imagen, de un vídeo o de una página web están sometidos a los derechos de autor y su utilización debe teóricamente ser objeto de una autorización previa.

Por ejemplo, YouTube avisa:

"verifique que todos los componentes de su vídeo son de su propia creación, incluida la parte de audio. Si usted utiliza, por ejemplo, una pista de audio cuyos derechos de autor son de una casa de discos que no dio la autorización para usarla, su vídeo puede atentar contra los derechos de autor de terceros y puede ser suprimido."

Y la página de copyright de Facebook contiene información sobre los derechos de propiedad intelectual relativos al contenido publicado en Facebook:

"Facebook respeta los derechos de propiedad intelectual de los autores y se compromete en ayudar a proteger sus derechos. Nuestra Declaración de derechos y responsabilidades impide a los usuarios publicar contenido que infrinja los derechos de propiedad intelectual de otro usuario o autor. Cuando recibimos una declaración válida de violación de los derechos de propiedad intelectual, suprimimos o prohibimos el acceso a los materiales en tela de juicio. También suprimimos las cuentas de los usuarios reincidentes".

ce unha solución alternativa aos autores que desexan liberar as súas obras, para permitirlles a outros usuarios reutilizalas e distribuílas, nun marco preciso (por exemplo: comercial, non comercial).

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

A identidade dixital é parte da nosa identidade como persoas, e como tal debe ser xestionada e coidade. Ao igual que nos preocupamos da saúde dos nosos fillos e fillas, pero non os fechamos na casa por medo a que enfermen, temos que preocuparnos pola súa identidade dixital, educándoos no uso das tecnoloxías, pero non debemos fecharnos a elas, é pouco recomendable e practicamente imposible.

La organización Creative Commons ofrece una solución alternativa a los autores que desean liberar sus obras, para permitirles a otros usuarios reutilizarlas y distribuirlas, en un marco preciso (por ejemplo: comercial, no comercial).

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

La identidad digital es parte de nuestra identidad como personas, y como tal debe ser gestionada y cuidada. Al igual que nos preocupamos de la salud de nuestros hijos y hijas, pero no los encerramos en la casa por miedo a que enfermen, tenemos que preocuparnos por su identidad digital, educándolos en el uso de las tecnologías, pero no debemos cerrarnos a ellas, es poco recomendable y prácticamente imposible.

ENRIQUE DANS

Profesor de Innovación en IE Business School desde o ano 1990. Tras licenciarse en Ciencias Biolóxicas pola USC, cursou un MBA no Instituto de Empresa, doutorouse en Sistemas de Información en UCLA, e desenvolveu estudos posdoutorais en Harvard Business School. No seu traballo como investigador, divulgador e asesor estuda os efectos da innovación tecnolóxica sobre as persoas, as empresas e a sociedade no seu conxunto. É colaborador habitual en numerosos medios de comunicación nacionais e internacionais en temas relacionados coa rede e a tecnoloxía, e escribe diariamente desde o ano 2003 na súa páxina persoal, enriquedans.com, unha das máis populares do mundo sobre innovación en lingua española.

Profesor de Innovación en IE Business School desde el año 1990. Tras licenciarse en Ciencias Biológicas por la USC, cursó un MBA en el Instituto de Empresa, se doctoró en Sistemas de Información en UCLA, y desarrolló estudios postdoctorales en Harvard Business School. En su trabajo como investigador, divulgador y asesor estudia los efectos de la innovación tecnológica sobre las personas, las empresas y la sociedad en su conjunto. Es colaborador habitual en numerosos medios de comunicación nacionales e internacionales en temas relacionados con la red y la tecnología, y escribe diariamente desde el año 2003 en su página personal, enriquedans.com, una de las más populares del mundo sobre innovación en lengua española.

Por que é importante acompañar os nosos fillos e as nosas fillas nas redes e na contorna dixital?

O importante é entender que ninguén nace sabendo. Cando nós eramos mozos xogábase en contornas nas que tamén che tiñan que explicar as normas de comportamento. Na rúa os nosos maiores explicábannos o funcionamento dos semáforos, as precaucións a tomar na beirarrúa e a calzada, e que por moito que che apetecese un caramelo non podías aceptalo de alguén que pasase por alí. Hoxe en día, por algunha misteriosa razón, pasamos a pensar que os nenos e as nenas nacen sabendo e que non é necesario explicar todas esas cousas, e iso non é certo en absoluto e ademais é unha idea moi perigosa. A idea de que os fillos e as fillas de hoxe xa veñen coa tecnoloxía prefixada no seu cerebro é falsa; creou unha xeración de nenos e nenas que non son nativos dixitais como se pretendía, senón orfos dixitais. E iso é moi perigoso.

Cal é o modelo ideal para aprender a manexarse en contornas dixitais?

O modo ideal de aprender a manexarse nunha contorna dixital é con experiencia; só se aprende con experiencia. O ideal é que a experiencia se vaia desenvolvendo nunha contorna onde os nenos e nenas se sintan acompañados polos seus pais

¿Por qué es importante acompañar a nuestros hijos y a nuestras hijas en las redes y en el entorno digital?

Lo importante es entender que nadie nace sabiendo. Cuando nosotros éramos jóvenes se jugaba en entornos en los que también te tenían que explicar las normas de comportamiento. En la calle nuestros mayores nos explicaban el funcionamiento de los semáforos, las precauciones a tomar en la acera y la calzada, y que por mucho que te apeteciese un caramelo no podías aceptarlo de alguien que pasase por allí. Hoy en día, por alguna misteriosa razón, hemos pasado a pensar que los niños y niñas nacen sabiendo y que no es necesario explicar todas esas cosas, y eso no es cierto en absoluto y además es una idea muy peligrosa. La idea de que los hijos e hijas de hoy ya vienen con la tecnología prefijada en su cerebro es falsa; ha creado una generación de niños y niñas que no son nativos digitales como se pretendía, sino huérfanos digitales. Y eso es muy peligroso.

¿Cuál es el modelo ideal para aprender a manejarse en entornos digitales?

El modo ideal de aprender a manejarse en un entorno digital es con experiencia; sólo se aprende con experiencia. Lo ideal es que la experiencia se vaya desarrollan-

e nais, pero non angustiados por eles. Por exemplo, procurar evitar o cuarto do computador, que é unha contorna onde será moi difícil estar con eles sen que sintan que estás a espreitalos. Racionalizar o uso dos dispositivos móbiles, loxicamente, non restrinxir enormemente o seu uso senón racionalizalo e tratar en todo momento de saber que están a facer os nosos nenos e nenas, da mesma maneira que o sabiamos cando xogaban en casa de amizades e lles preguntabamos a que xogaban, que facían, etc. O símil é exacto.

Que habilidades de futuro relacionadas coa identidade dixital debería dominar a mocidade?

O ideal é entender que a contorna dixital é unha contorna que ten as súas propias regras e as súas propias ferramentas de construción. Se pensamos que os nosos fillos e fillas van ser simplemente usuarios estamos a adoptar unha a mentalidade moi cortoplacista. A contorna dixital vai desenvolver moitas oportunidades para facer actividades múltiples, de feito, case todas as actividades poderanse realizar nesa contorna, pero tamén para construír e desenvolver esa contorna. Temos que entender que os nosos fillos e fillas non deberían ser só usuarios, deberían entender estas ferramentas. Non deben ser só usuarios dun smartphone, deben entender como funciona e por que funciona. Deben entender que hai dentro dun computador e por que funciona, e idealmente deben ter como mínimo una certa cultura de programación, aínda que sexa simplemente saber que é un bucle, que é un condicional, que é unha definición de variables... unas poucas cousas mínimas, pero entender as regras de como se constrúe esa contorna.

Se puideses dar un único consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

O importante é crear familiaridade coa canle. A rede, como todas as contornas, ten os seus protocolos: canto antes empecen e canto máis eduquemos eses protocolos, mellor e máis consistentemente será o seu desenvolvemento. Ensinar ás nenas e nenos a peneirar información, a participar con respecto, a utilizar as canles para o que son, a xestionar a súa privado en un entorno en el que los niños y las niñas se sientan acompañados por sus padres y madres, pero no agobiados por ellos. Por ejemplo, procurar evitar la habitación del ordenador, que es un entorno en que será muy difícil estar con ellos sin que sientan que estás mirándoles por encima del hombro. Racionalizar el uso de los dispositivos móviles, lógicamente, no restringir enormemente su uso sino racionalizarlo y tratar en todo momento de saber qué están haciendo nuestros niños y niñas, de la misma manera que lo sabíamos cuando jugaban en casa de amistades y les preguntábamos a qué jugaban, qué hacían, etc. El símil es exacto.

¿Qué habilidades de futuro relacionadas con la identidad digital debería dominar la juventud?

Lo ideal es entender que el entorno digital es un entorno que tiene sus propias reglas y sus propias herramientas de construcción. Si pensamos que nuestros hijos e hijas van a ser simplemente usuarios estamos adoptando una a mentalidad muy cortoplacista. El entorno digital va a desarrollar muchas oportunidades para hacer actividades múltiples, de hecho, casi todas las actividades se podrán realizar en ese entorno, pero también para construir y desarrollar ese entorno. Tenemos que entender que nuestros hijos y nuestras hijas no deberían ser solo usuarios, deberían entender estas herramientas. No deben ser solo usuarios o usuarias de un smartphone, deben entender cómo funciona y por qué funciona. Deben entender qué hay dentro de un ordenador y por qué funciona, e idealmente deben tener como mínimo una cierta cultura de programación, aunque sea simplemente saber qué es un bucle, qué es un condicional, qué es una definición de variables... unas pocas cosas mínimas, pero entender las reglas de cómo se construye ese entorno.

Si pudieras dar un único consejo a familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Lo importante es crear familiaridad con el canal. La red, como todos los entornos, tiene sus protocolos: cuanto antes empiecen y cuanto más eduquemos esos protocolos, mejor y más consistentemen-

cidade ou a comportarse con educación e sentido común é tan importante como o desenvolver normas de seguridade: sen xerar histerias, pero explicando os riscos. En realidade, non ten demasiadas diferenzas co que facían as familias hai anos para ensinar a saír á rúa, ou a comportarse en casas alleas: simplemente esixe tomarse un certo interese, documentarse un pouco, e aplicar o sentido común.

te se desarrollarán. Enseñar a los niños y niñas a tamizar información, a participar con respeto, a utilizar los canales para lo que son, a gestionar su privacidad o a comportarse con educación y sentido común es tan importante como el desarrollar normas de seguridad: sin generar histerias, pero explicando los riesgos. En realidad, no tiene demasiadas diferencias con lo que hacían las familias hace años para enseñar a salir a la calle, o a comportarse en casas ajenas: simplemente exige tomarse un cierto interés, documentarse un poco, y aplicar el sentido común.

MARCUS FERNÁNDEZ

Con formación en Informática, desenvolve a súa actividade profesional no mundo da Internet, participando en iniciativas pioneiras na Rede galega, así como no asociacionismo (ISOC-GAL, EGANET e a Asociación PuntoGal), o que o levou a contribuír á posta en marcha do dominio de Internet para a sociedade galega (o .gal). Exerce funcións de administración e redacción da web de Código Cero (diario de novas tecnolóxicas de Galicia, con edición mensual en papel) dende 2001, o que combinou con preto de 3 anos nunha experiencia de televisión local en Compostela. Complementa a súa actividade profesional cun blog persoal (Marcus.gal) e distintas colaboración en medios galegos (Tempos Novos, Luzes, RadioVoz, Radio Coruña-Cadena SER, Radio Galega e Televisión de Galicia).

Con formación en Informática, desarrolla su actividad profesional en el mundo de la Internet, participando en iniciativas pioneras en la Red gallega, así como en el asociacionismo (ISOC-GAL, EGANET y la Asociación PuntoGal), lo que le llevó a contribuir en la puesta en marcha del dominio de Internet para la sociedad gallega (el .gal). Ejerce funciones de administración y redacción de la web de Código Cero (diario de noticias tecnológicas de Galicia, con edición mensual en papel) desde 2001, que combinó cerca de 3 años con una experiencia de televisión local en Compostela. Complementa su actividad profesional con un blog personal (Marcus.gal) y distintas colaboraciones en medios gallegos (Tempos Novos, Luzes, RadioVoz, Radio Coruña-Cadena SER, Radio Galega y Televisión de Galicia).

Que é a identidade dixital e o *personal branding*? Como se xestiona de xeito eficaz?

Os conceptos de identidade dixital e marca persoal están moi ligados. A identidade dixital é esencialmente a pegada que deixamos na Rede, de xeito que cando alguén busque información sobre a nosa persoa, vaise facer unha idea de como somos segundo o rastro que deixamos en liña.

Debido a que actualmente as plataformas de redes sociais son as principais fontes de información, resulta evidente que as persoas tomamos cada vez un rol máis activo na creación dos contidos que serven de espello da nosa persoa, e precisamente aí temos o *personal branding* ou marca persoal, que vén a ser todo o que facemos para manter o control sobre a nosa identidade dixital.

É moi importante ser conscientes de que todo o que publicamos en Internet pode contribuír á imaxe que o resto de usuarios e usuarias terán de nós: desde fotografías e vídeos até un comentario nun contexto pouco afortunado. Pero é igual de importante entender que todo o que se fai público en liña está fóra do noso control, e unha vez que hai copias de contidos fóra do noso computador ou teléfono xa non podemos volver atrás, e aínda que os

¿Qué es la identidad digital y el *personal branding*? ¿Cómo se gestiona de manera eficaz?

Los conceptos de identidad digital y marca personal están muy ligados. La identidad digital es esencialmente la huella que dejamos en la Red, de suerte que cuando alguien busque información sobre nuestra persona, se hará una idea de cómo somos según el rastro que dejamos en línea.

Dado que actualmente las plataformas de redes sociales son las principales fuentes de información, resulta evidente que las personas tomamos cada vez un rol más activo en la creación de los contenidos que sirven de espejo de nuestra persona, y precisamente ahí tenemos el *personal branding* o marca personal, que viene a ser todo lo que hacemos para mantener el control sobre nuestra identidad digital.

Es muy importante ser conscientes de que todo lo que publicamos en Internet puede contribuir a la imagen que el resto de usuarios y usuarias tendrán de nosotros y de nosotras: desde fotografías y vídeos hasta un comentario en un contexto poco afortunado. Pero es igual de importante entender que todo lo que se hace público en línea está fuera de nuestro control, y una vez que hay copias de contenidos fuera de nuestro ordenador

borremos non poderemos estar seguros e seguras de se non hai copias a circular pola Rede. Iso débenos facer reflexionar no feito de que a mellor estratexia de marca persoal é ter moi clara a pegada que queremos deixar na Rede, potenciando sempre a imaxe que queremos dar ao público, e sendo moi conscientes de cando estamos a movernos en esferas privadas ou públicas: non podemos dicir o mesmo nun chío de Twitter que pode ler todo o mundo que nunha conversa que manteñamos cun amigo ou amiga ou familiar en WhatsApp. A Internet non é a barra dun bar, senón unha fiestra ao mundo; é o meirande escaparate que unha persoa pode ter, tanto para establecer relacións persoais como profesionais.

O mellor consello que se pode dar á hora de querer controlar a identidade dixital é pensar sempre antes de publicar algo na Rede e, cando queiramos compartir cousas de carácter moi persoal, temos que manter certo control sobre a configuración de privacidade das distintas plataformas en liña: intercambiar fotografías dunha festa con amigos e amigas pode estar ben, pero debemos evitar que sexa algo que poida ver calquera, xa que podería transmitir a imaxe de que somos unha persoa sen compromiso co seu traballo.

Que é a *infoxicación*? Como se debe contrastar a información en Internet?

O concepto de *infoxicación* pretende recoller o problema do exceso de información, algo que pode aplicarse tanto a temáticas moi específicas como á información xeral que nos axuda a tomar decisións para o noso día a día.

En Internet a sobrecarga informativa pode chegar de moitos xeitos, que vai desde os contidos repetidos ou derivados que non achegan información nova (aínda que si consumen o noso tempo), até a cantidade de información molesta e inservible (publicidade, correo lixo...) á que temos que facer fronte ao navegar pola web ou ler o correo electrónico.

De xeito moi xeral podemos entender que o exceso de información principalmente fai que perdamos produtividade, pois para poder obter coñecemento temos que peneirar moitos contidos; pero desta *infoxicación* tamén temos un efecto perverso moi negativo: moita da información está incompleta ou incluso é errónea,

o teléfono ya no podemos volver atrás, y aunque los borremos no podremos estar seguros o seguras de que no hay copias circulando por la Red. Eso nos debe hacer reflexionar sobre el hecho de que la mejor estrategia de marca personal es tener muy clara la huella que queremos dejar en la Red, potenciando siempre la imagen que queremos dar en público, y siendo muy conscientes de cuando estamos moviéndonos en esferas personales o públicas: no podemos decir lo mismo en un tweet de Twitter que puede leer todo el mundo que en una conversación que mantengamos con un amigo o una amiga o algún familiar en WhatsApp. Internet no es la barra de un bar, sino una ventana al mundo; es el mayor escaparate que una persona pueda tener, tanto para establecer relaciones personales como profesionales.

El mejor consejo que puede darse en el momento de querer controlar la identidad digital es pensar siempre antes de publicar algo en la Red y, cuando queramos compartir cosas de carácter muy personal tenemos que mantener cierto control sobre la configuración de privacidad de las distintas plataformas en línea: intercambiar fotografías de una fiesta con amigos y amigas puede estar bien, pero debemos evitar que sea algo que pueda ver cualquier persona, ya que podría transmitir la imagen de que somos una persona sin compromiso con su trabajo.

¿Qué es la *infoxicación*? ¿Cómo se debe contrastar la información en Internet?

El concepto de *infoxicación* pretende recoger el problema del exceso de información, algo que puede aplicarse tanto a temáticas muy específicas como a la información general que nos ayuda a tomar decisiones para nuestro día a día.

En Internet la sobrecarga informativa puede llegar de muchas maneras, que va desde los contenidos repetidos o derivados que no aportan información nueva (aunque sí consumen nuestro tiempo), hasta la cantidad de información molesta e inservible (publicidad, correo basura...) a la que tenemos que hacer frente al navegar por la web o leer el correo electrónico.

De manera muy general podemos entender que el exceso de información principalmente hace que perdamos productividad,

facendo moi complicado chegar a unha conclusión útil.

Canta máis información teñamos, máis difícil será buscar entre ela, debullar os datos de interese e, especialmente, poder discernir a verdade entre informacións manipuladas, comentarios persoais e moitas outras manifestacións que incluso poden estar elaboradas como broma e que ao sacarse de contexto poden levar a engano. Temos así que cultivar o pensamento crítico e contrastar as informacións importantes do mellor xeito posible.

O primeiro no que temos que fixarnos cando recibimos unha información dubidosa é na súa fonte (por exemplo, non é o mesmo ler unha nova nun xornal coñecido que nunha rede social ou incluso nunha mensaxe de WhatsApp) e procurar buscar fontes adicionais (os artigos poden conter ligazóns para ampliar a información, confirmándoa ou incluso invalidándoa ao terse rectificado a nova na que se baseou o texto que estamos a ler).

Tamén resulta moi importante fixarse na data das novas (xa que a información pode estar obsoleta), especialmente diante da posibilidade de que a información sexa unha broma (o que pode intuírse se a data de publicación é o 28 de decembro ou o 1 de abril, ou se a cabeceira é un medio humorístico como ElMundoToday.com).

Outro elemento a ter moi en conta é a autoría da información, xa que diso dependerá moito a credibilidade. Saber quen escribe unha nova tamén axuda moito a coñecer a existencia de inclinacións de distinto tipo desa persoa (como a súa ideoloxía política).

Pero diante de dúbida o mellor probablemente sexa preguntar a unha persoa experta: perante síntoma dunha enfermidade temos que consultar a un doutor ou unha doutora e non ao buscador de Google.

Que é a *netiqueta* e cales son as súas regras básicas?

A *netiquette* ou *netiqueta* é unha palabra que fai referencia ao conxunto de normas de comportamento xeral en Internet, ou sexa, adaptación da *etiqueta* tradicional á Rede, buscando favorecer a convivencia das persoas usuarias. Estas normas aplícanse nos moitos ámbitos que existen

pues para poder obtener conocimiento tenemos que cribar muchos contenidos; pero de esta i*nfoxicación* también tenemos un efecto perverso muy negativo: mucha de la información está incompleta o incluso es errónea, haciendo muy complicado llegar a una conclusión útil.

Cuanta más información tengamos, más difícil será buscar entre la misma, desgranar los datos de interés y, especialmente, poder discernir la verdad entre informaciones manipuladas, comentarios personales y muchas otras manifestaciones que incluso pueden estar elaboradas en broma y al sacarse de contexto pueden llevar a engaño. Tenemos así que cultivar el pensamiento crítico y contrastar las informaciones importantes de la mejor manera posible.

Lo primero en lo que tenemos que fijarnos cuando recibimos una información dudosa es de su fuente (por ejemplo, no es lo mismo leer una noticia en un periódico conocido que en una red social o incluso en un mensaje de WhatsApp) e intentar buscar fuentes adicionales (los artículos pueden contener enlaces para ampliar la información, confirmándola o incluso invalidándola al haberse rectificado la noticia en la que se basó el texto que estamos leyendo).

También resulta muy importante fijarse en la fecha de las noticias (ya que la información puede estar obsoleta), especialmente ante la posibilidad de que la información sea una broma (lo que puede intuirse si la fecha de publicación es el 28 de diciembre o el 1 de abril, o si la cabecera es un medio humorístico como ElMundoToday.com).

Otro elemento a tener muy en cuenta es la autoría de la información, pues de eso dependerá mucho la credibilidad. Saber quien escribe una noticia también ayuda mucho a conocer la existencia de inclinaciones de distinto tipo de esa persona (como su ideología política).

Pero ante la duda lo mejor probablemente sea preguntar a una persona experta: ante un síntoma de una enfermedad tenemos que consultar a un doctor o a una doctora y no al buscador de Google.

¿Qué es la *netiqueta* y cuáles son sus reglas básicas?

La *netiquette* o *netiqueta* es una palabra que hace referencia al conjunto de nor-

en Internet, pero non están carentes de certas dificultades para a súa adopción como son o feito de que non estean recollidas formalmente ou que estean en constante evolución (teñen que adaptarse aos hábitos da meirande parte de quen as emprega).

Inicialmente a *netiqueta* estaba presente principalmente como unha serie de normas para o uso do correo electrónico que viñan do uso do correo tradicional, como redactar mensaxes que comezasen cun saúdo e rematasen cunha despedida e cunha sinatura, pero iso tamén levou á creación de excepcións (por exemplo, non resulta agradable que unha sinatura teña un tamaño superior ao da mensaxe neta). Tamén se recomenda que no asunto dos correos electrónicos se dea conta da temática tratada na mensaxe dun xeito moi breve, pero entendendo ese elemento fóra da mensaxe en si (quero dicir, que non se deben formular preguntas no asunto que precisen resposta, pois dificultaría a súa redacción). Tamén habería outras formas de cortesía como non remitir documentos adxuntos que non fosen solicitados e moderar o seu tamaño sempre que sexa posible, xa que existen limitacións importantes neste sentido en moitas plataformas de correo electrónico.

Pero este tipo de instrucións básicas tamén poden aplicarse aos foros (nos que hai que comportarse seguindo as normas establecidas polos seus administradores e administradoras ou, simplemente, mantendo o mesmo ton que o resto de persoas interlocutoras), nas bitácoras de Internet (debemos evitar facer comentarios nunha entrada dun blog que se afasten da temática do artigo), nos sistemas de chat (normalmente hai que cinguirse a temáticas específicas e evitar acaparar os espazos de comunicación)... e incluso cada plataforma de redes sociais teñen normas de seu, que van desde manter a cortesía no trato até a utilización de determinadas imaxes como avatar da nosa conta de usuario ou usuaria. Trátase simplemente de manter un comportamento civilizado no que a persoa usuaria poña mentalmente cara ás persoas coas que está a interactuar na Rede, para manter así un nivel de cortesía que si tería con esas mesmas persoas nun trato cara a cara.

mas de comportamiento general en Internet, o sea, adaptación de la *etiqueta* tradicional a la Red, buscando favorecer la convivencia de las personas usuarias. Estas normas se aplican a los muchos ámbitos que existen en Internet, pero no están carentes de ciertas dificultades para su adopción, como son el hecho de que no estén recogidas formalmente o que estén en constante evolución (tienen que adaptarse a los hábitos de la mayor parte de quien las usa).

Inicialmente la *netiqueta* estaba presente principalmente como una serie de normas para el uso del correo electrónico que venían del uso del correo tradicional, como redactar mensajes que comenzaran saludando y acabaran con una despedida y una firma, pero eso también llevó a la creación de excepciones (por ejemplo, no resulta agradable que una firma tenga un tamaño superior al del mensaje neto). También se recomienda que en el asunto de los correos electrónicos se dé cuenta de la temática tratada en el mensaje de una manera muy breve, pero entendiendo ese elemento fuera del mensaje en sí (o sea, que no se deben formular preguntas en el asunto que necesiten respuesta, pues dificultaría la redacción de la misma). También habría otras formas de cortesía como no remitir documentos adjuntos que no fueran solicitados y moderar su tamaño siempre que sea posible, ya que existen limitaciones importantes a tal respeto en muchas plataformas de correo electrónico.

Pero este tipo de instrucciones básicas también pueden aplicarse a los foros (en los que hay que comportarse siguiendo las normas establecidas por sus administradores y administradoras o, simplemente, manteniendo el mismo tono que el resto de interlocutores e interlocutoras), en las bitácoras de Internet (debemos evitar hacer comentarios en una entrada de un blog que se alejen de la temática del artículo), en los sistemas de chat (normalmente hay que ceñirse a temáticas específicas y evitar acaparar los espacios de comunicación)... e incluso cada plataforma de redes sociales tiene normas de por sí, que van desde mantener la cortesía en el trato hasta la utilización de determinadas imágenes como avatar de nuestra cuenta de usuario. Se trata simplemente de mantener un comportamiento civilizado en el que la persona usuaria ponga mentalmen-

Que é o *karma* en Internet? Como funcionan os sistemas baseados na reputación?

En Internet existen diferentes plataformas nas que os usuarios e as usuarias teñen un nivel de reputación establecido que en moitos casos se coñece como *karma,* e que serve así para que o resto de usuarios e usuarias poida coñecer o nivel de credibilidade dunha persoa ou tamén para que os sistemas automáticos dean unha maior visibilidade aos usuarios e usuarias mellor valorados.

Cando entramos en sistemas de recomendacións de novas como Menéame ou Chuza, as persoas usuarias poden compartir ligazóns de Internet para a súa discusión e difusión, e os comentarios que se fan ao redor de cada un destes contidos poden valoralos negativa ou positivamente todos os usuarios e todas as usuarias, de xeito que os comentarios máis votados serán máis visibles. Os usuarios e as usuarias que compartan as mellores historias e publiquen os mellores comentarios irán gañando puntos de *karma,* de xeito que as súas contribucións futuras terán unha valoración inicial superior, mentres que os usuarios e as usuarias que teñan un comportamento tóxico ou que queiran aproveitarse do sistema para facer publicidade atoparán puntuacións negativas para disuadilos e disuadilas das súas prácticas.

Isto mesmo tamén se pode aplicar en plataformas de compra-venda, de xeito que quen compra e quen vende recibe valoracións que irán construíndo unha reputación para que no futuro as outras persoas que queiran facer negocios con eles saiban se son de fiar.

Estes mecanismos de control teñen como eivas principais a mala recepción de novas persoas usuarias, xa que nun principio será difícil que un novato ou unha novata teña credibilidade, e a proliferación de grupos de usuarios e usuarias que poden abusar do seu elevado nivel de *karma* conxunto creando o que poderían considerarse liñas editoriais, pervertendo en boa medida o espírito inicial dos sistemas de edición non xerárquica (nos que se traslada o rol de selección dos contidos ás propias persoas usuarias) como os mencionados.

¿Qué es el *karma* en Internet? ¿Cómo funcionan los sistemas basados en la reputación?

En Internet existen diferentes plataformas en las que los usuarios y las usuarias tienen un nivel de reputación establecido que en muchos casos se conoce como *karma,* y que sirve así para que el resto de usuarios y usuarias pueda conocer el nivel de credibilidad de una persona o también para que los sistemas automáticos den una mayor visibilidad a los usuarios y usuarias mejor valorados.

Cuando entramos en sistemas de recomendaciones de noticias como Menéame o Chuza, las personas usuarias pueden compartir enlaces de Internet para su discusión y difusión, y los comentarios que se hacen alrededor de cada uno de estos contenidos pueden valorarlos negativa o positivamente todos los usuarios y todas las usuarias, de suerte que los comentarios más votados serán más visibles. Los usuarios y las usuarias que compartan las mejores historias y publiquen los mejores comentarios irán ganando puntos de *karma,* de suerte que sus contribuciones futuras tendrán una valoración inicial superior, mientras que los usuarios y las usuarias que tengan un comportamiento tóxico o que quieran aprovecharse del sistemas para hacer publicidad encontrarán puntuaciones negativas para disuadirlos o disuadirlas de sus prácticas.

Esto incluso también puede aplicarse en plataformas de compra-venta, de suerte que quien compra y quien vende recibe valoraciones que irán construyendo una reputación para que en el futuro otras personas que quieran hacer negocios con ellos sepan si son de fiar.

Estos mecanismos de control tienen como principales defectos la mala recepción de nuevas personas usuarias, ya que en un principio será difícil que un novato o una novata tenga credibilidad, y la proliferación de grupos de usuarios y usuarias que pueden abusar de su elevado nivel de *karma* conjunto creando lo que podrían considerarse líneas editoriales, pervirtiendo en buena medida el espíritu inicial de los sistemas de edición no jerárquica

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Sobre a identidade dixital coido que o mellor que podemos facer é instar a pensar a longo prazo e ser conscientes de que non somos donos nin donas das identidades alleas. Temos que ser moi respectuosos e respectuosas coas imaxes dos menores e das menores, e ter claro desde o primeiro momento que as persoas adultas teñen que velar pola súa protección.

Se botamos a vista atrás seguro que máis dun ou dunha sentiu humillación cando nunha visita familiar se botou man dun vello álbum de fotografías no que se reflectían momentos dos que cada quen podía non estar orgulloso ou orgullosa por distintos motivos. Pero esas sesións realizábanse no ámbito doméstico! Temos que ser conscientes que agora os álbums fotográficos se constrúen día a día dun xeito moito máis público, polo que temos que controlar ao máximo a información que compartimos de menores, para que poidan ser eles mesmos e elas mesmas quen decida o que queren facer coa súa identidade dixital no futuro.

Cómpre protexer os mozos e as mozas de hoxe para que poidan ser as persoas adultas do mañá do xeito máis libre posible.

(en los que se traslada el rol de selección de los contenidos a las propias personas usuarias) como los mencionados.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Sobre la identidad digital creo que lo mejor que podemos hacer es instar a pensar a largo plazo y ser conscientes de que no somos dueños o dueñas de las identidades ajenas. Tenemos que ser muy respetuosos e respetuosas con las imágenes de los y las menores, y tener claro desde el primer momento que las personas adultas tienen que velar por su protección.

Si echamos la vista atrás seguro que más de uno o de una sintió humillación cuando en una visita familiar se echó mano de un viejo álbum de fotografías en el que se reflejaban momentos de los que uno o una podía no estar orgulloso/a por distintos motivos. ¡Pero esas sesiones se realizaban en el ámbito doméstico! Tenemos que ser conscientes de que ahora los álbumes fotográficos se construyen día a día de una manera mucho más pública, por lo que tenemos que controlar al máximo la información que compartimos de menores, para que puedan ser ellos mismos y ellas mismas quienes decidan que quieren hacer con su identidad digital en el futuro.

Hace falta proteger a los chicos y a las chicas de hoy para que puedan ser las personas adultas del mañana de la manera más libre posible.

JUAN J. FERNÁNDEZ GARCÍA

Presidente da asociación TADEGa (Tecnoloxías de Atención á Diversidade na Educación Galega), mestre, titor e secretario do CEIP "Juan Fernández Latorre" da Coruña. Anteriormente, director de proxectos e asesor TIC na Consellería de Educación. Posgrao en telecomunicacións e Internet.

Presidente de la asociación TADEGa (Tecnologías de Atención a la Diversidad en la Educación Gallega), maestro, tutor y secretario del CEIP "Juan Fernández Latorre" de A Coruña. Anteriormente, director de proyectos y asesor TIC en la Consellería de Educación. Postgrado en telecomunicaciones e Internet.

Como debería ser o uso dos dispositivos móbiles nos centros educativos?

Hoxe isto supón na escola un cambio de métodos e conceptos máis importante, lento e difícil do que parece. De feito en moitas escolas non está permitido traer móbiles da casa coa escusa da problemática das redes sociais no recinto escolar (entre outras). E se non están permitidos para que poñerse a analizar como usalos?

Ademais o alumnado menor non ten, moitas veces, o necesario acompañamento educativo no seu uso, nin por parte das familias, nin por parte da estrutura escolar, resultando unha actividade autodidacta, desatendida e consumista ás agochadas e sen criterios de madurez, que reduce o seu uso a xoguetes de consumo e parladoiros ás agochadas.

É urxente desandar ese camiño, e é difícil cunha parte do alumnado carente de adultos de referencia no dixital (nin por parte da familia nin por parte da escola).

Como ademais o uso dos servizos máis interesantes (NFC, acelerómetros, calidade da pantalla, etc.) están só dispoñibles nos dispositivos de gama alta, non sempre accesibles ás familias de economías máis humildes, a sistematización dun bo aproveitamento de todas as capacidades destes dispositivos pasará por usar dispositivos do centro e non os persoais. Nese senso, sería máis que necesario que os actuais equipos Abalar deixaran de ser PC de escritorio e fosen dispositivos móbiles tipo tablet (ou mixto en todo caso). Baixo esa condición, teríamos acceso a aprendizaxes, interiorización e aproveitamentos máis acordes ao que debe ser e con opción a espallar esta óptica ás estruturas familiares que tamén o precisen.

¿Cómo debería ser el uso de los dispositivos móviles en los centros educativos?

Hoy esto supone en la escuela un cambio de métodos y conceptos más importante, lento y difícil de lo que parece. De hecho, en muchas escuelas no está permitido traer móviles de casa con la excusa de la problemática de las redes sociales en el recinto escolar (entre otras). Y si no están permitidos, ¿para que ponerse a analizar cómo usarlos?

Además, el alumnado menor no tiene, muchas veces, el necesario acompañamiento educativo en su uso, ni por parte de las familias, ni por parte de la estructura escolar, resultando una actividad autodidacta, desatendida y consumista a escondidas y sin criterios de madurez, que reduce su uso a juguetes de consumo y chats a escondidas.

Es urgente desandar ese camino, y es difícil con una parte del alumnado carente de personas adultas de referencia en lo digital (ni por parte de la familia ni por parte de la escuela).

Como además el uso de los servicios más interesantes (NFC, acelerómetros, calidad de la pantalla, etc.) están solo disponibles en los dispositivos de gama alta, no siempre accesibles a las familias de economías más humildes, la sistematización de un buen aprovechamiento de todas las capacidades de estos dispositivos pasará por usar dispositivos del centro y no los personales. En ese sentido, sería más que necesario que los actuales equipos Abalar dejasen de ser PC de escritorio y fuesen dispositivos móviles tipo tableta (o mixto en todo caso). Bajo esa condición, tendríamos acceso a aprendizajes, interiorización y aprovechamientos más acordes a lo que debe ser y con opción

En resumo: alta necesidade, máxima urxencia e importantes dificultades á vista. Todo un reto.

Por que é importante formar cidadáns dixitalmente competentes?

Non é importante, é imprescindible: os cativos que hoxe educamos e formamos vivirán nun futuro laboral e social que non somos capaces hoxe de prever, imaxinar e concretar. Seranlles esixidas capacidades, coñecementos e destrezas que non son, maioritariamente, as que hoxe lles brindamos. O que si sabemos é que as súas destrezas e competencias dixitais serán un factor decisivo da súa vida laboral e, incluso, no seu ámbito persoal e social.

Sería imperdoable que o alumnado de hoxe quedase relegado no seu futuro por causa de que as únicas destrezas que posúe son as de ser meros consumidores de produtos dixitais carentes de todo sentido crítico, e acadadas pola súa conta ás nosas costas. Estarán presentes nesa rede dixital e nós somos responsables de que aprendan a madurar e a ser cidadáns libres e creativos dentro das mesmas redes e usándoas, e non como simples consumidores.

Que posibilidades dá Internet para o crecemento do alumnado como persoas a nivel persoal e profesional?

Hoxe moita poboación adulta usa a Rede como escaparate de consumo e como lugar no que dar vía libre aos egos. Con esa óptica, nada invitaría a sacarlle proveito nas aulas. En cambio, as posibilidades reais, se as sabemos aproveitar, son outras ben distintas, mesmo opostas.

Como docentes temos 2 obrigas irrenunciables: achegar ao alumnado un uso máis útil, responsable e crítico, e facer que descubran as moitas opcións de creación, colaboración, innovación e sentido crítico.

Estás aprendizaxes, nunca serán espontáneas nin inmediatas; requiren de práctica, atención e tempo; e pasan necesariamente por un acompañamento e guiado dos seus mundos adultos de referencia (escola e familia) para modificar, entre outras cousas, os esquemas herdados previos de individualismo consumista e do resultado inmediato e irreflexivo.

a diseminar esta óptica a las estructuras familiares que también lo necesiten.

En resumen: alta necesidad, máxima urgencia e importantes dificultades a la vista. Todo un reto.

¿Por qué es importante formar ciudadanos y ciudadanas digitalmente competentes?

No es importante, es imprescindible: los niños y niñas que hoy educamos y formamos vivirán en un futuro laboral y social que no somos capaces de prever, imaginar y concretar. Les serán exigidas capacidades, conocimientos y destrezas que no son, mayoritariamente, las que hoy les brindamos. Lo que sí sabemos es que sus destrezas y competencias digitales serán un factor decisivo de su vida laboral e, incluso, en su ámbito personal y social.

Sería imperdonable que el alumnado actual quedase relegado en su futuro por causa de que las únicas destrezas que posee son las de ser meras personas consumidoras de productos digitales carentes de todo sentido crítico, y conseguidas por su cuenta a nuestras espaldas. Estarán presentes en esa red digital y somos responsables de que aprendan a madurar y a ser personas libres y creativas dentro de las mismas redes, usándolas, no como simples consumidoras.

¿Qué posibilidades da Internet al crecimiento del alumnado como personas a nivel personal y profesional?

Hoy mucha población adulta usa la Red como escaparate de consumo y como lugar en el que dar vía libre a los egos. Con esa óptica, nada invitaría a sacarle provecho en las aulas. En cambio, las posibilidades reales, si las sabemos aprovechar, son otras bien distintas, incluso contrarias.

Como docentes tenemos dos deberes irrenunciables: acercar al alumnado un uso más útil, responsable y crítico, y hacer que descubran las muchas opciones de creación, colaboración, innovación y sentido crítico.

Estos aprendizajes nunca serán espontáneos ni inmediatos; requieren de práctica, atención y tiempo; y pasan necesariamente por un acompañamiento y guía de sus mundos adultos de referencia (escue-

Modificando estes parámetros e cando podemos avanzar no resto.

Que están a supor as tecnoloxías dixitais na vida das persoas con diversidade funcional?

Lamentablemente a realidade é moi negativa. Por cada oportunidade brindada aos colectivo de persoas con diversidade funcional, avánzase 10 veces máis nos restantes. A maiores, a Rede e os seus servizos tratan ás persoas con diversidade funcional como a un colectivo aparte, minoritario e non rendible. Resultado: moito discurso de boa fe e paternal pero tramposo e discriminador.

A accesibilidade de contidos, servizos e ferramentas é de obrigado cumprimento por lei (Real Decreto 1494/2007, BOE de 21/11/2007) 10 anos despois desta norma, máis do 90% da rede segue sendo inaccesible a persoas con discapacidade (diversidade funcional). Exposto este problema nos foros de deseño e creación, e mesmo nas propias universidades, as desculpas seguen a ser as mesmas: falta de recursos, dificultade de transformar o xa feito inaccesible en accesible, colectivos minoritarios, etc. Cando neste momento máis do 90% dos contidos e servizos web teñen datas de creación posteriores á normativa.

Ser minoría implica ter dereito a violala? Pensamos algunha vez que a discapacidade será, seguro, unha realidade nalgún momento das nosas vidas? Quen nos deu permiso para decidir sobre a vida, as oportunidades e o destino doutras persoas só porque teñan capacidades diferentes das nosas?

Como é posible axudar a outros a través de Internet. Que medios de participación social existen?

Curiosamente, se facemos unha procura en Google co texto *"educación y participación social"* o primeiro documento titúlase *"Educación y participación social de la infancia"* (tempo de traballo apenas uns segundos) na súa síntese queda clara unha evidencia: non se trata de falar ou de estudar sistemas de participación social, entre outros motivos, porque a infancia percibe como *"incomprensible, absurdo e inmodificable o mundo que está máis alá das súas contornas máis inmediatas como a familia e a escola"* (cousa que maioritariamente tamén lle acontece aos adul-

la y familia) para modificar, entre otras cosas, los esquemas heredados previos de individualismo consumista y del resultado inmediato e irreflexivo.

Modificando estos parámetros es cuando podemos avanzar en el resto.

¿Qué están suponiendo las tecnologías digitales en la vida de las personas con diversidad funcional?

Lamentablemente la realidad es muy negativa. Por cada oportunidad brindada a los colectivos de personas con diversidad funcional, se avanza diez veces más en los restantes. Además, la Red y sus servicios tratan a las personas con diversidad funcional como a un colectivo aparte, minoritario y no rentable. Resultado: mucho discurso de buena fe y paternal pero tramposo y discriminador.

La accesibilidad de contenidos, servicios y herramientas es de obligado cumplimiento por ley (Real Decreto 1494/2007, BOE de 21/11/2007). Diez años después de esta norma, más del 90% de la Red sigue siendo inaccesible a personas con discapacidad (diversidad funcional). Expuesto este problema en los foros de diseño y creación, e incluso en las propias universidades, las disculpas siguen siendo las mismas: falta de recursos, dificultad de transformar lo ya hecho inaccesible en accesible, colectivos minoritarios, etc., cuando hoy por hoy más del 90% de los contenidos y servicios web tienen fechas de creación posteriores a la normativa.

¿Ser minoría implica tener derecho a violarla? ¿Pensamos alguna vez que la discapacidad será, seguro, una realidad en algún momento de nuestras vidas? ¿Quién nos ha dado permiso para decidir sobre la vida, las oportunidades y el destino de otras personas solo porque tengan capacidades diferentes de las nuestras?

¿Cómo es posible ayudar a otras personas a través de Internet? ¿Qué medios de participación social existen?

Curiosamente, si hacemos una búsqueda en Google con el texto *"educación y participación social"* el primer documento se titula *"Educación y participación social de la infancia"* (tiempo de trabajo, apenas unos segundos). En su síntesis queda

tos) polo que o único xeito de progresar é: participar real e directamente en Consellos infantís ou mediante outros xeitos de participación en diversos proxectos (se non se experiencia, a teoría resulta *«kafkiana»*). Polo tanto, o reto non está en facer unha procura en Internet sobre sistemas de participación (apenas décimas de segundo), nin no proceso de filtrado posterior (de pouca validez no tempo xa que os resultados cambian a cada pouco). O reto está en vertebrar nas aulas, nos centros e nos barrios sistemas que permitan realmente esta participación.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Todas e todos temos dereito pleno a ser e a estar con dignidade na escola, na casa, na rúa... e os nosos fillos e alumnos tamén. Ata aí todo claro. ¿E o dereito a ser e a estar con dignidade na Rede Dixital? Quedóusenos atrás? Un dereito ademais, que non está para ser gardado nun caixón, senón para ser defendido e coidado cada día.

Os nosos fillos e alumnos, vulnerables ademais, precisan acompañamento, coidado, apoio e protección na rede; un acompañamento para transitar a unha vida adulta e madura.

É a nosa obriga e a nosa responsabilidade.

clara una evidencia: no se trata de hablar o de estudiar sistemas de participación social, entre otros motivos, porque la infancia percibe como *"incomprensible, absurdo e inmodificable el mundo que está más allá de sus entornos más inmediatos como la familia y la escuela"* (cosa que mayoritariamente también le sucede a las personas adultas) por lo que la única manera de progresar es: participar real y directamente en consejos infantiles o mediante otras maneras de participación en diversos proyectos (si no se experiencia, la teoría resulta *«kafkiana»*). Por lo tanto, el reto no está en hacer una búsqueda en internet sobre sistemas de participación (apenas décimas de segundo), ni en el proceso de filtrado posterior (de poca validez en el tiempo ya que los resultados cambian a cada instante). El reto está en vertebrar en las aulas, en los centros y en los barrios sistemas que permitan realmente esta participación.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Todas y todos tenemos derecho pleno a ser y a estar con dignidad en la escuela, en la casa, en la calle... y nuestros hijos e hijas y alumnado también. Hasta ahí todo claro. ¿Y el derecho a ser y a estar con dignidad en la Red Digital? ¿Se nos ha quedado atrás? Un derecho, además, que no está para ser guardado en un cajón, sino para ser defendido y cuidado cada día.

Nuestros hijos e hijas y alumnado, vulnerables, además, precisan acompañamiento, cuidado, apoyo y protección en la Red; un acompañamiento para transitar a una vida adulta y madura.

Es nuestro deber y nuestra responsabilidad.

Mª CARMEN FERNÁNDEZ MORANTE

Profesora Titular de Didáctica e Organización Escolar da Universidade de Santiago de Compostela e Doutora en Ciencias da Educación.

Decana da Facultade de Ciencias da Educación da USC.

Especialista en Tecnoloxía Educativa. A súa traxectoria profesional vincúlase á formación en TIC aplicadas á formación, impartindo materias universitarias como Tecnoloxía Educativa, Novas Tecnoloxías Aplicadas á Educación, Educación en Medios e Web Social ou Investigación en e-learning, e cursos de formación e innovación docente neste campo para profesorado de todos os niveis educativos e outros profesionais da educación.

Pertence ao Grupo de investigación de Tecnoloxía Educativa da USC (GI-1438).

Profesora Titular de Didáctica y Organización Escolar de la Universidad de Santiago de Compostela y Doctora en Ciencias de la Educación.

Decana de la Facultad de Ciencias de la Educación de la USC.

Especialista en Tecnología Educativa. Su trayectoria profesional se vincula a la formación en TIC aplicadas a la formación, impartiendo materias universitarias como Tecnología Educativa, Nuevas Tecnologías Aplicadas a la Educación, Educación en Medios y Web Social o Investigación en e-learning, y cursos de formación e innovación docente en este campo para profesorado de todos los niveles educativos y otros profesionales de la educación.

Pertenece al Grupo de investigación de Tecnología Educativa de la USC (GI-1438).

Como debería ser o uso dos dispositivos móbiles nos centros educativos?

En primeiro lugar, deberiamos preguntarnos: que tipo de dispositivos móbiles poden ser de utilidade nas aulas? Fundamentalmente, as tabletas. A respecto disto, dúas consideracións previas para reflexionar en como usalas:

- A primeira, que nos centros educativos deben utilizarse **dispositivos institucionais, non persoais,** para garantir con iso que todo o alumnado –independentemente do seu poder adquisitivo e recursos familiares– ten acceso e posibilidade de uso no proceso de aprendizaxe e, fundamentalmente, nos centros educativos.
- A segunda, que nos centros educativos debe traballarse con todo tipo de dispositivos móbiles e non limitarse a unha marca, sistema operativo ou tipo exclusivamente xa que debemos preparar o alumnado para desenvolverse tamén fóra da aula e fóra dela van dispor dun abanico amplo de tecnoloxías. Debemos ensinar a traballar cun determinado medio como é a tableta independentemente da marca ou do siste-

¿Cómo debería ser el uso de los dispositivos móviles en los centros educativos?

En primer lugar, deberíamos plantearnos ¿qué tipo de dispositivos móviles pueden ser de utilidad en las aulas? Fundamentalmente las tabletas. Respecto a esto, dos consideraciones previas a plantear cómo usarlas:

- La primera, que en los centros educativos deben utilizarse dispositivos institucionales, no personales, para garantizar con ello que todo el alumnado -independientemente de su poder adquisitivo y recursos familiares- tiene acceso y posibilidad de uso en su proceso de aprendizaje y fundamentalmente en los centros educativos.
- La segunda, que en los centros educativos debe trabajarse con todo tipo de dispositivos móviles y no limitarse a una marca, sistema operativo o tipo exclusivamente pues debemos prepararles para desenvolverse también fuera del aula y fuera de ella van a disponer de un abanico amplio de tecnologías. Debemos enseñar a trabajar con un determinado medio como es la tableta independientemente de la marca o sistema

ma operativo. Non facelos cativos ou dependentes dun determinado modelo.

A partir disto, non podemos obviar unha problemática ou dilema ao que calquera docente e centro se vai expor que é a presenza de teléfonos **móbiles ou o acceso a estes dispositivos por parte do alumnado**, especialmente menores, e que xera grandes distorsións (vulnerabilidade por exposición continuada, disrupción na aula, adicción á conectividade nalgúns casos, problemas de atención...). Neste sentido entendo, e esta é unha mensaxe para as familias, que un neno ou unha nena non necesita un teléfono móbil para estar permanentemente localizado/conectado. Un menor ou unha menor cando está no centro está seguro e custodiado e baixo a responsabilidade de profesionais. É importante entender que para utilizar de forma responsable e construtiva este tipo de dispositivos, o menor ou a menor debe estar preparado ou preparada e non é conveniente facilitalos como medios persoais a idades temperás.

No que se refire agora ao **uso nos centros dos dispositivos móbiles, o alumnado debe aprender, sen dúbida, a utilizar estas tecnoloxías desde idades temperás e de forma responsable** co que implican de conexión, comunicación, posibilidades de creación e de apoio ao proceso de aprendizaxe. A isto referímonos cando falamos de competencia dixital e esta competencia debe abordarse explícita e directamente no currículo. Non soamente de forma transversal xa que require dunha formación específica. É importante formar para un bo uso, é dicir:

- Un uso **diversificado** dos medios (diversidade de medios, diversidade de usos educativos nos procesos de ensino-aprendizaxe, diversidade de aplicacións/servizos).
- **Orientado ao proceso de aprendizaxe:** comunicación e colaboración con outros, acceso a contidos educativos, posibilidades de creación e expresión de ideas e coñecementos (multilinguaxes/multialfabetización). É dicir, sempre en función dun propósito ou obxectivo de aprendizaxe.
- **Equilibrado** no que se refire á capacidade de autorregulación dos tempos e das interaccións presenciais e virtuais.

operativo. No hacerles cautivos o dependientes de un determinado modelo.

Dicho esto, no podemos obviar una problemática o dilema que cualquier docente y centro van a plantearse y que es la presencia de teléfonos **móviles o el acceso a estos por parte del alumnado,** especialmente menores, y que genera grandes distorsiones (vulnerabilidad por exposición continuada, disrupción en el aula, adicción a la conectividad en algunos casos, problemas de atención...). En este sentido entiendo, y este es un mensaje para las familias, que un niño o una niña no necesita un teléfono móvil para estar permanentemente localizado/conectado. Un menor o una menor cuando está en el centro está seguro y custodiado y bajo la responsabilidad de profesionales. Es importante entender que para utilizar de forma responsable y constructiva este tipo de dispositivos, el menor o la menor ha de estar preparado o preparada y no es conveniente facilitarlos como medios personales a edades tempranas.

En lo que se refiere ahora al uso en los centros de los dispositivos móviles, el alumnado debe aprender a utilizar estas tecnologías sin duda desde edades tempranas y de forma responsable con lo que implican de conexión, comunicación, posibilidades de creación y de apoyo al proceso de aprendizaje. A esto nos referimos cuando hablamos de competencia digital y esta debe abordarse explícita y directamente en el currículo. No solamente de forma transversal pues requiere una formación específica. Es importante formar para un buen uso, es decir:

- Un uso **diversificado** de los medios (diversidad de medios, diversidad de usos educativos en los procesos de enseñanza-aprendizaje, diversidad de aplicaciones/servicios).
- **Orientado al proceso de aprendizaje:** comunicación y colaboración con otros, acceso a contenidos educativos, posibilidades de creación y expresión de ideas y conocimientos (multilenguajes/multialfabetización). Es decir, siempre en función de un propósito u objetivo de aprendizaje.
- **Equilibrado** en lo que se refiere a la capacidad de autorregulación de los tiempos y de las interacciones presenciales y virtuales.

- E **seguro,** isto é, conscientes dos riscos que comporta e capaz de previlos e afrontalos.

Que posibilidades dá Internet para o crecemento do alumnado como persoas a nivel persoal e profesional?

Eu creo que, en xeral, tense **mitificado Internet** e atribúeselle unha capacidade formativa que en si mesma este medio non ten. De feito, se nos fixamos nos discursos fálase das súas posibilidades de aprendizaxe sen referencia algunha ao papel indispensable do profesorado, como se Internet por si mesma tivese capacidade de xerar aprendizaxes. Isto non é certo. Son formulacións superficiais e incluso frívolas e irresponsables polos riscos que comportan.

Dito isto, e partindo da base de que o papel do profesorado é imprescindible para facer de Internet un recurso para a aprendizaxe, e que isto require dun tempo de dedicación pola súa parte importante dentro e fóra da aula, este medio ofrece moitas posibilidades ao alumnado a nivel persoal e educativo. Fundamentalmente resúmense en tres:

- A posibilidade de acceder **a grandes cantidades de información e moi diversificada** que provén de persoas, institucións e grupos. Neste sentido Internet é unha fonte moi rica coa condición de que o alumnado saiba (e para iso hai que formalo; non se aprende por ensaio-erro) dirixir, filtrar, seleccionar e tratar a información até elaborar o seu propio coñecemento. É dicir, sempre que o alumnado teña criterio, capacidade de contextualizar a información e de ter unha visión global. A isto referímonos con formar en competencias informacionais.
- A posibilidade de acceder **a persoas, grupos e experiencias moi diversas e de carácter globalizado** (non só ás máis próximas). Internet neste sentido permite comunicarse, debater, achegar e compartir ideas, crear cousas xuntos... Estamos a falar de cooperar para resolver problemas e actividades educativas, establecer redes para a aprendizaxe e o lecer. É dicir, xerar comunidades de aprendizaxe. Obviamente isto require unha orientación, guía e supervisión destes procesos polo profesorado.

- Y **seguro,** es decir, consciente de los riesgos que comporta y capaz de prevenirlos y afrontarlos.

¿Qué posibilidades da Internet al crecimiento del alumnado como personas a nivel personal y profesional?

Yo creo que en general se ha **mitificado Internet** y se le atribuye una capacidad formativa que en sí misma este medio no tiene. De hecho, si nos fijamos en los discursos se habla de sus posibilidades de aprendizaje sin referencia alguna al papel indispensable del profesorado, como si Internet por si misma tuviera capacidad de generar aprendizajes. Esto no es cierto. Son planteamientos superficiales e incluso frívolos e irresponsables por los riesgos que comportan.

Dicho esto, y partiendo de la base de que el papel del profesorado es imprescindible para hacer de Internet un recurso para el aprendizaje, y que esto requiere un tiempo de dedicación por su parte importante dentro y fuera del aula, este medio ofrece muchas posibilidades al alumnado a nivel personal y educativo. Fundamentalmente se resumen en tres:

- La posibilidad de acceder **a grandes cantidades de información y muy diversificada** que proviene de personas, instituciones y grupos. En este sentido Internet es una fuente muy rica, siempre y cuando el alumnado sepa (y para eso hay que formarlo, no se aprende por ensayo-error) dirigir, filtrar, seleccionar y tratar la información hasta elaborar su propio conocimiento. Es decir, siempre que el alumnado tenga criterio, capacidad de contextualizar la información y de tener una visión global. A esto nos referimos con formar en competencias informacionales.
- La posibilidad de acceder **a personas, grupos y experiencias muy diversas y de carácter globalizado** (no solo las más próximas). Internet en este sentido permite comunicarse, debatir, aportar y compartir ideas, crear cosas juntos... Estamos hablando de cooperar para resolver problemas y actividades educativas, establecer redes para el aprendizaje y el ocio. Es decir, generar comunidades de aprendizaje. Obviamente esto requiere una orientación, guía y supervisión de estos procesos por el profesorado.

- A posibilidade de acceder **a múltiples e cambiantes ferramentas e servizos** (especialmente derivados da Web Social) de indubidable utilidade no proceso de aprendizaxe e nas relacións persoais e actividades de lecer. Referímonos a ferramentas de creación mesmo colectiva, de difusión e publicación de contidos, de colaboración etc. cada vez máis accesibles sen custo algún nin requirir de equipos de altas prestacións.

Que é a *infoxicación*? Como se debe contrastar a información en Internet?

Alfons Cornella (especialista en ciencias da información) acuñou este termo para facer referencia á intoxicación informativa derivada do exceso de información dispoñible actualmente e á incapacidade para procesala correctamente.

Para min esa **exposición a inxentes cantidades de información** en Internet (e nos medios de comunicación en xeral que hoxe converxen na Rede) **sen habilidades para procesala** correctamente supón un risco importante e débese fundamentalmente a dous factores:

- O exceso de información por falta **de capacidade para buscar e xestionala** (que tamén se chama desbordamento) ao non saber seleccionar e procesar tanta como hai á disposición hoxe en día.
- E a **presenza elevada e camuflada de información "tóxica",** non veraz, sen rigor, tendenciosa, de baixa ou nula credibilidade á que todos e todas, e especialmente o alumnado, estamos expostos e expostas. A posibilidade que deu Internet (especialmente a Web Social) á cidadanía de acceso e de difusión multicanle multiplicou a información dispoñible pero tamén esvaeceu ou fai difícil discriminar a súa validez e orixe. Desta forma atopámonos con todo tipo de información e con información que eu denomino "tóxica" porque:
  - En ocasións obedece a unha intención de manipular (descontextualizando as ideas, ofrecendo visións parciais e nesgadas e aproveitando o inmediato das redes sociais).
  - Opínase/publícase moitas veces desde o descoñecemento ou a falta de rigor. Hoxe en día as redes amplificaron as posibilidades de expre-

- La posibilidad de acceder a **múltiples y cambiantes herramientas y servicios** (especialmente derivados de la Web Social) de indudable utilidad en el proceso de aprendizaje y en las relaciones personales y actividades de ocio. Nos referimos a herramientas de creación incluso colectiva, de difusión y publicación de contenidos, de colaboración etc. cada vez más accesibles sin coste alguno ni requerir equipos de altas prestaciones.

¿Qué es la *infoxicación*? ¿Cómo se debe contrastar la información en Internet?

Alfons Cornella (especialista en ciencias de la información) acuñó este término para hacer referencia a la intoxicación informativa derivada del exceso de información disponible actualmente y la incapacidad para procesarla correctamente.

Para mi, esa **exposición a ingentes cantidades de información** en Internet (y en los medios de comunicación en general que hoy convergen en la Red) **sin habilidades para procesarla** correctamente supone un riesgo importante y se debe fundamentalmente a dos factores:

- El exceso de información por falta **de capacidad para buscar y gestionarla** (que también se llama desbordamiento) al no saber seleccionar y procesar tanta como hay a disposición hoy en día.
- Y la **presencia elevada y camuflada de información "tóxica",** no veraz, sin rigor, tendenciosa, de baja o nula credibilidad a la que todos y todas, y especialmente el alumnado, estamos expuestos y expuestas. La posibilidad que ha dado Internet (especialmente la Web Social) a la ciudadanía de acceso y de difusión multicanal ha multiplicado la información disponible pero también ha desdibujado o hace difícil discriminar su validez y origen. De esta forma nos encontramos con todo tipo de información y con información que yo denomino "tóxica" porque:
  - Obedece en ocasiones a una intención de manipular (descontextualizando las ideas, ofreciendo visiones parciales y sesgadas y aprovechando la inmediatez de las redes sociales).

sarse e isto ás veces confúndese coa idea de que "todo o mundo sabe de todo" e emítense opinións superficiais, infundadas e mesmo apoiadas en erros.

- As canles de distribución en Internet impiden ás veces facer unha "trazabilidade" da información e, polo tanto, recoñecer a súa orixe.
- As tecnoloxías actuais, e en especial as redes sociais, permiten esconder as identidades (anonimato das persoas emisoras) e con iso responsabilizarse dos contidos publicados.

A partir disto, a pregunta é: como se debe contrastar a información? Dúas cuestións básicas:

1. **Coñecendo a natureza das diferentes fontes de información e o seu grao de credibilidade.** É dicir, ensinando a discriminalas e facilitando -o profesorado- diversas fontes de busca solventes (con organismos e persoas solventes detrás). O alumnado debe coñecer como son ou non son os procesos de filtro, por exemplo, de ferramentas como Wikipedia ou de diferentes centros de recursos dixitais, da RAE, da biblioteca nacional... Aprender a identificar fontes solventes.
2. **Tendo criterios para valorar a información atopada e que significa.** Que está a indicar?, contrastala con outras, analizar a súa procedencia. En definitiva, falamos de dúas competencias transversais que deben abordarse seriamente na educación obrigatoria e en todas as materias do currículo: alfabetización informacional e pensamento crítico.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Educar desde a infancia na responsabilidade e no coidado da imaxe propia na Rede á que acceden desde diferentes dispositivos e en diferentes situacións (educativas e de lecer). Refírome á perda de control sobre os datos persoais, aos riscos de manipulación e distorsión, á vulnerabilidade diante de condutas delituosas que poden causar danos persoais (*ciberbullying, sexting, sextorsión...*) etc.

Ensinar a pensar antes de actuar. Alertar o alumnado do inmediato das tecnoloxías e da facilidade coa que nos levan a ex-

- Se opina/publica muchas veces desde el desconocimiento o la falta de rigor. Hoy en día las redes han amplificado las posibilidades de expresarse y esto se confunde a veces con la idea de que "todo el mundo sabe de todo" y se emiten opiniones superficiales, infundadas e incluso apoyadas en errores.
- Los canales de distribución en Internet impiden a veces hacer una "trazabilidad" de la información y por tanto reconocer el origen de la misma.
- Las tecnologías actuales, y en especial las redes sociales, permiten esconder las identidades (anonimato de las personas emisoras) y con ello responsabilizarse de los contenidos publicados.

Dicho esto, la pregunta es: ¿cómo se debe contrastar la información? Dos cuestiones básicas:

1. **Conociendo la naturaleza de las diferentes fuentes de información y su grado de credibilidad.** Es decir, enseñando a discriminarlas y facilitando -el profesorado- diversas fuentes de búsqueda solventes (con organismos y personas solventes detrás). El alumnado debe conocer cómo son o no son los procesos de filtro, por ejemplo, de herramientas como Wikipedia o de diferentes centros de recursos digitales, la RAE, la biblioteca nacional... Aprender a identificar fuentes solventes.
2. **Teniendo criterios para valorar la información encontrada y qué significa.** ¿Qué está indicando?, contrastarla con otras, analizar su procedencia. En definitiva, hablamos de dos competencias transversales que deben abordarse seriamente en la educación obligatoria y en todas las materias del currículo: alfabetización informacional y pensamiento crítico.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Educar desde la infancia en la responsabilidad y el cuidado de la imagen de uno mismo en la Red a la que acceden desde diferentes dispositivos y en diferentes situaciones (educativas y de ocio). Me refiero a la pérdida de control sobre

por datos persoais (e da nosa contorna social) que permanecen, sobre os que perdemos o control unha vez emitidos e que poden facernos vulnerables, utilizarse con propósitos alleos.

Axudarlles a desenvolver habilidades de uso das tecnoloxías que lles permitan previr, identificar e afrontar con seguridade os riscos aos que nos expomos cando utilizamos as tecnoloxías, especialmente Internet ou calquera aplicación que se apoie nela.

Dous consellos neste sentido:

- **Preparar para iso antes da adolescencia.** É o momento en que nos escoitan e están receptivos (aos adultos). Despois buscan outros referentes entre os seus iguais. Explicar o por que e como utilizar correctamente as tecnoloxías. Falar sobre os riscos. Hai moitos exemplos e páxinas web con recursos de calidade para abordalo. Por exemplo www.pantallasamigas.net
- Profesorado e familias deben **actuar coordinadas e ser coherentes** nas súas formulacións.

los datos personales, a los riesgos de manipulación y distorsión, a la vulnerabilidad ante conductas delictivas que pueden causar daños personales (*ciberbullying, sexting, sextorsión…*) etc.

Enseñar a pensar antes de actuar. Alertar al alumnado de la inmediatez de las tecnologías y de la facilidad con la que nos llevan a exponer datos personales (y de nuestro entorno social) que permanecen, sobre los cuáles perdemos el control una vez emitidos y que pueden hacernos vulnerables, utilizarse con propósitos ajenos.

Ayudarles a desarrollar habilidades de uso de las tecnologías que les permitan prevenir, identificar y afrontar con seguridad los riesgos a los que nos exponemos cuando utilizamos las tecnologías, especialmente Internet o cualquier aplicación que se apoye en ella.

Dos consejos en este sentido:

- **Preparar para ello antes de la adolescencia.** Es el momento en que nos escuchan y están receptivos (a los adultos). Luego buscan otros referentes entre sus iguales. Explicar el porqué y cómo utilizar correctamente las tecnologías. Hablar sobre los riesgos. Hay muchos ejemplos y páginas web con recursos de calidad para abordarlo. Por ejemplo www.pantallasamigas.net
- Profesorado y familias deben **actuar coordinadas en esto y ser coherentes** en sus planteamientos.

JOSÉ JULIO FERNÁNDEZ RODRÍGUEZ

Profesor titular de dereito constitucional da USC e antigo Valedor do Pobo.

Director do Centro de Estudios de Seguridade da USC. Posúe seis titulacións superiores, incluído o doutoramento. Ampla produción científica, de elevado impacto, que inclúe diversos traballos sobre Internet e dereitos fundamentais e o control de contidos na rede.

Profesor titular de derecho constitucional de la USC y antiguo Valedor del Pueblo.

Director del Centro de Estudios de Seguridad de la USC. Posee seis titulaciones superiores, incluido el doctorado. Amplia producción científica, de elevado impacto, que incluye diversos trabajos sobre Internet y derechos fundamentales y el control de contenidos en la red.

Cal é o mellor modo de previr condutas nocivas en Internet?

Faise necesario efectuar unha precisión previa: pódese diferenciar entre dous tipos de contidos problemáticos, os contidos ilícitos e os nocivos. Os ilícitos son os contidos contrarios ao ordenamento xurídico de referencia. Entre outros destacan os de tipo delituoso. Á súa vez, os contidos nocivos son legais, pero resultan prexudiciais (desde un punto de vista social, ético ou moral) para certo sector da poboación, como a mocidade ou a infancia. O réxime duns e doutros debe ser diferente, tendo en conta, en todo caso, que non se debe prohibir en Internet o que está permitido noutros medios de comunicación. O contido nocivo de por si non se pode prohibir xa que pode estar amparado pola liberdade de expresión ou creación artística. Do que se trata é de evitar o acceso a estes contidos ao colectivo que se vería prexudicado.

Dito isto, a resposta a esta pregunta pódese abordar desde dúas ópticas, que resultan compatibles e que se poden empregar conxuntamente. Por unha banda, a óptica educativa e, por outra, a perspectiva técnica informática.

Así as cousas, desde as estratexias educativas hai que salientar a dignidade da persoa e a necesidade de respectar o próximo. Trátase de transmitirlle aos e ás menores que a liberdade e o lexítimo lecer deben servir para a propia realización persoal e para a socialización saudable. En cambio, divertirse con accións nocivas prexudica na medida en que normaliza condutas e valores cos que só debe enfrontarse unha persoa adulta. Os rapa-

¿Cuál es el mejor modo de prevenir conductas nocivas en Internet?

Se hace necesario efectuar una precisión previa: se puede diferenciar entre dos tipos de contenidos problemáticos, los contenidos ilícitos y los nocivos. Los ilícitos son los contenidos contrarios al ordenamiento jurídico de referencia. Entre ellos destacan los de tipo delictivo. A su vez, los contenidos nocivos son legales, pero resultan perjudiciales (desde un punto de vista social, ético o moral) para cierto sector de la población, como la juventud o la infancia. El régimen de unos y de otros debe ser diferente, teniendo en cuenta, en todo caso, que no se debe prohibir en Internet lo que está permitido en otros medios de comunicación. El contenido nocivo por sí mismo no se puede prohibir puesto que puede estar amparado por la libertad de expresión o creación artística. De lo que se trata es de evitar el acceso al mismo al colectivo que se vería perjudicado.

Dicho esto, la respuesta a esta pregunta se puede abordar desde dos ópticas, que resultan compatibles y que se pueden emplear conjuntamente. Por un lado, la óptica educativa y, por otro, la perspectiva técnica informática.

Así las cosas, desde las estrategias educativas hay que enfatizar la dignidad de la persona y la necesidad de respetar al prójimo. Se trata de transmitir a los y las menores que la libertad y el legítimo ocio deben servir para la propia realización personal y para la sana socialización. En cambio, divertirse con acciones nocivas les perjudica en la medida en que normaliza conductas y valores con los que solo

ces e as rapazas teñen que saber que a súa formación se realiza por etapas, que non se deben anticipar para non perder eficacia. O valor da responsabilidade e a recomendación da cautela van axudar niso. Isto é, concienciar ao e á menor de que o contido nocivo son prexudiciais na súa socialización.

Ademais, tamén desde a educación se debe mostrar o perigo do descontrol de Internet. E ligar este perigo ao que indicabamos antes sobre o respecto ao próximo e sobre o valor da propia responsabilidade.

Por outra banda, distintos recursos técnicos informáticos resultan imprescindibles para evitar o acceso a contido nocivo. Especialmente, software de control parental (no fogar e nos colexios) actualizado e eficaz; e fomento da etiquetaxe web para saber de antemán o perfil de idade recomendado de acceso á correspondente web.

En Internet, existen as fronteiras?

Internet, a Rede de redes de carácter mundial, tivo repercusións en todos os ámbitos da acción humana. Tamén no referente ás fronteiras tradicionais, debedoras da evolución da Historia política e, en gran parte, asentadas conceptualmente desde a Paz de Westfalia.

Os procesos supranacionais, sobre todo en Europa, relativizaron as fronteiras no Vello Continente, tanto a través da Unión Europea como por efecto do Consello de Europa, aínda que neste último caso en menor medida.

Con todo, o gran cambio conceptual xeopolítico foi a tecnoloxía dixital, que permitiu a creación de Internet. Se deixamos agora de lado a evolución pasada desta Rede, hoxe en día presenta un marcado carácter global que non coñece fronteiras. Ou case, porque é certo que algún país se esforza por manter o control territorial de Internet, e con relativo éxito (China, Turquía por momentos, monarquías árabes en ocasións...). É dicir, nas nacións democráticas o funcionamento de Internet, baseado no hipertexto creador de hiperligazóns e a súa tendencia crecente a crear e gardar contidos na "nube", deu lugar a unha verdadeira globalización que non coñece fronteiras. Pero en países autoritarios o control territorial aínda existe.

debe enfrentarse una persona adulta. Los chavales y las chavalas tienen que saber que su formación se realiza por etapas, que no se deben anticipar para no perder eficacia. El valor de la responsabilidad y la recomendación de la cautela ayudarán en ello. O sea, concienciar al o a la menor de que el contenido nocivo les perjudica en su socialización.

Además, también desde la educación debe mostrarse el peligro del descontrol de Internet. Y ligar este peligro a lo que indicábamos antes sobre el respeto al prójimo y sobre el valor de la propia responsabilidad.

Por otra parte, distintos recursos técnicos informáticos resultan imprescindibles para evitar el acceso al contenido nocivo. Especialmente, software de control parental (en el hogar y en los colegios) actualizado y eficaz; y fomento del etiquetado web para saber de antemano el perfil de edad recomendado de acceso a la correspondiente web.

En Internet, ¿existen las fronteras?

Internet, la Red de redes de carácter mundial, ha tenido repercusiones en todos los ámbitos de la acción humana. También en lo referente a las fronteras tradicionales, deudoras de la evolución de la Historia política y, en gran parte, asentadas conceptualmente desde la Paz de Westfalia.

Los procesos supranacionales, sobre todo en Europa, relativizaron las fronteras en el Viejo Continente, tanto a través de la Unión Europea como por efecto del Consejo de Europa, aunque en este último caso en menor medida.

Sin embargo, el gran cambio conceptual geopolítico ha sido la tecnología digital, que ha permitido la creación de Internet. Dejando ahora de lado la evolución pasada de esta Red, hoy en día presenta un marcado carácter global que no conoce fronteras. O casi, porque es cierto que algún país se esfuerza por mantener el control territorial de Internet, y con relativo éxito (China, Turquía por momentos, monarquías árabes en ocasiones...). Es decir, en las naciones democráticas el funcionamiento de Internet, basado en el hipertexto creador de hipervínculos y su tendencia creciente a crear y guardar contenidos en la "nube", ha dado lugar a una verdadera globalización que no co-

Isto non significa que non haxa control en Internet, nin que non deba habelo. O control existe, aínda que con máis dificultade que no mundo analóxico. E debe existir nun contexto como o actual de tantas ameazas á seguridade e á intimidade. Á marxe da autorregulación que ás veces tentan os grandes provedores de acceso e contidos e o ente administrativo de asignación de dominios (ICANN), os distintos ordenamentos xurídicos aplícanse cando se pode probar unha actividade en determinado territorio sometido a ese ordenamento, sobre todo cando se trata de cuestións penais ou tributarias. É dicir, o ordenamento xurídico aplícase cando se dan os supostos para iso (principio de legalidade), independentemente de se estamos no mundo analóxico e dixital. Naquel será máis fácil actuar e probar os sucesos, e neste máis complicado, ao esixir unha abordaxe específica e especializada que ás veces non se consegue.

Que debemos facer de atoparmos contido non axeitado (pedofilia, incitación ao odio, violencia extrema...) en Internet?

Faise necesario precisar o sentido da pregunta. Simplificando, como xa se dixo anteriormente, pódese dicir que existen dous tipos de contidos inadecuados: os ilícitos e os nocivos. Os ilícitos son os contidos contrarios ao ordenamento xurídico de que se trate, como os de tipo delituoso. En cambio, os nocivos non son ilegais senón prexudiciais para certo tipo de poboación (como menores, por exemplo). A pedofilia é en todo o Dereito Comparado un contido ilícito; en cambio a violencia extrema parece un simple contido nocivo.

Diante dos contidos ilícitos hai que efectuar a denuncia ao órgano público competente, normalmente as forzas e os corpos de seguridade do Estado ou os xulgados de garda. Iso pode facerse de maneira presencial nos cuarteis, comisarías ou xulgados; ou de forma dixital nas páxinas web das forzas de seguridade, cando é posible. Ademais, a Policía Nacional ten unha unidade especializada no mundo dixital, a Brigada de Investigación Tecnolóxica (https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html); e na Garda Civil atopamos o Grupo de Delitos

noce fronteras. Pero en países autoritarios el control territorial aún existe.

Esto no significa que no haya control en Internet, ni que no deba haberlo. El control existe, aunque con más dificultad que en el mundo analógico. Y debe existir en un contexto como el actual de tantas amenazas a la seguridad y a la intimidad. Al margen de la autorregulación que a veces intentan los grandes proveedores de acceso y contenidos y el ente administrativo de asignación de dominios (ICANN), los distintos ordenamientos jurídicos se aplican cuando se puede probar una actividad en determinado territorio sometido a ese ordenamiento, sobre todo cuando se trata de cuestiones penales o tributarias. Es decir, el ordenamiento jurídico se aplica cuando se dan los supuestos para ello (principio de legalidad), independientemente de si estamos en el mundo analógico y digital. En aquel será más fácil actuar y probar los sucesos, y en este más complicado, exigiendo un abordaje específico y especializado que a veces no se consigue.

¿Qué debemos hacer si encontramos contenido inapropiado (pedofilia, incitación al odio, violencia extrema...) en Internet?

Se hace necesario precisar el sentido de la pregunta. Simplificando, como ya se dijo anteriormente, se puede decir que existen dos tipos de contenidos inadecuados: los ilícitos y los nocivos. Los ilícitos son los contenidos contrarios al ordenamiento jurídico de que se trate, como los de tipo delictivo. En cambio, los nocivos no son ilegales sino perjudiciales para cierto tipo de población (como menores, por ejemplo). La pedofilia es en todo el Derecho Comparado un contenido ilícito; en cambio la violencia extrema parece un simple contenido nocivo.

Ante los contenidos ilícitos hay que efectuar la denuncia al órgano público competente, normalmente las fuerzas y cuerpos de seguridad del Estado o los juzgados de guardia. Ello puede hacerse de manera presencial en los cuarteles, comisarías o juzgados; o de forma digital en las páginas web de las fuerzas de seguridad, cuando es posible. Además, la Policía Nacional tiene una unidad especializada en el mundo digital, la Brigada de Investigación Tecnológica (https://www.

Telemáticos (https://www.gdt.guardiacivil.es/webgdt/home_alerta.php).

É importante concienciar a todo o mundo da necesidade de denunciar para poder acabar cos delitos e, polo tanto, cos contidos ilícitos. Neste sentido aínda falta compromiso, polo que hai que apelar a unha maior sensibilización da sociedade. Agora iso é especialmente relevante, cando a democracia está a loitar contra radicalismos violentos, como o yihadismo, que empregan Internet como instrumento esencial de propaganda.

Outra cousa sucederá se o contido é simplemente nocivo para os e as menores (como a pornografía entre persoas adultas, as apostas, a violencia que non supoña delito...). Diante deste contido é do que se deben articular as opcións informáticas existentes para impedir o acceso, como o software de control parental actualizado e eficaz, e a etiquetaxe web, e desenvolver estratexias educativas específicas para explicarlle aos e ás menores que eses contidos resultan prexudiciais para a súa adecuada socialización.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Sobre todo, educación. Explícome.

As familias e o profesorado deben estar moi atentos e atentas na formación dos e das menores na tecnoloxía dixital. Internet e as redes sociais son a xanela ao mundo, á comunicación e á socialización. Esta tarefa formativa require dun requisito previo de suma importancia: as persoas adultas teñen que posuír os coñecementos adecuados para levar adiante ese ensino. Un problema relevante en Galicia, e constatado a través de enquisas, é o parcial analfabetismo dixital de moitas persoas adultas, o que implica unha auténtica brecha cos seus fillos e fillas, moito máis coñecedores e coñecedoras das cuestións dixitais. Así será imposible un control razoable e unha formación correcta sobre as fortalezas e debilidades da tecnoloxía dixital.

Polo tanto, resumindo, o consello sería: as persoas titulares da patria potestade e o profesorado deben ter unha formación dixital sólida para ensinar o positivo e o negativo desa tecnoloxía aos e ás menores. E un segundo consello (aínda que só se pedía un): ese ensino debe ser propor-

policia.es/org_central/judicial/udef/bit_quienes_somos.html); y en la Guardia Civil encontramos el Grupo de Delitos Telemáticos (https://www.gdt.guardiacivil.es/webgdt/home_alerta.php).

Es importante concienciar a todo el mundo de la necesidad de denunciar para poder acabar con los delitos y, por ende, con los contenidos ilícitos. En este sentido, todavía falta compromiso, por lo que hay que apelar a una mayor sensibilización de la sociedad. Ahora esto es especialmente relevante, cuando la democracia está luchando contra radicalismos violentos, como el yihadismo, que emplean Internet como instrumento esencial de propaganda.

Otra cosa sucederá si el contenido es simplemente nocivo para los y las menores (como la pornografía entre personas adultas, las apuestas, la violencia que no suponga delito...). Ante este contenido se deben articular las opciones informáticas existentes para impedir el acceso, como el software de control parental actualizado y eficaz, y el etiquetado web, y desarrollar estrategias educativas específicas para explicar a los y a las menores que esos contenidos resultan perjudiciales para su adecuada socialización.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Ante todo, educación. Me explico.

Las familias y el profesorado deben estar muy atentos y atentas en la formación de los y las menores en la tecnología digital. Internet y las redes sociales son la ventana al mundo, a la comunicación y socialización. Esta tarea formativa requiere un requisito previo de suma importancia: las personas adultas tienen que poseer los conocimientos adecuados para llevar a cabo esa enseñanza. Un problema relevante en Galicia, y constatado a través de encuestas, es el parcial analfabetismo digital de muchas personas adultas, lo que implica una auténtica brecha con sus hijos e hijas, mucho más conocedores y conocedoras de las cuestiones digitales. Así será imposible un control razonable y una formación correcta sobre las fortalezas y debilidades de la tecnología digital.

Por lo tanto, resumiendo, el consejo sería: las personas titulares de la patria potestad y el profesorado deben tener una

cional e equilibrado, sen esaxeracións, fomentando o espírito crítico e a responsabilidade.

Deste xeito, na estratexia educativa relativa á identidade dixital hai que transmitirlle ao e á menor que cada ser humano é único e irrepetible e que debe construír a súa personalidade respectando os dereitos das demais persoas. E todo iso, desde a tolerancia e o compromiso cidadán. Como o que entra en Internet é moi difícil que desapareza, hai que sensibilizar ao e á menor nunha actitude de cautela e precaución, que valore e saliente a súa personalidade, a súa intimidade e imaxe. Todos os elementos físicos e psicolóxicos, emotivos, cognitivos e de conduta serven para conformar a complexidade inherente a cada persoa. Por esta razón, até que poida asumir de adulto ou adulta as súas decisións con maior liberdade e coñecemento, o ou a menor debe protexer os seus elementos constitutivos para non expolos no labirinto sen saída da Rede.

sólida formación digital para enseñar lo positivo y lo negativo de esa tecnología a los y las menores. Y un segundo consejo (aunque solo se pedía uno): esa enseñanza debe ser proporcional y equilibrada, sin exageraciones, fomentando el espíritu crítico y la responsabilidad.

De este modo, en la estrategia educativa relativa a la identidad digital, hay que transmitir al y a la menor que cada ser humano es único e irrepetible, y que debe construir su personalidad respetando los derechos de las demás personas. Y todo ello, desde la tolerancia y el compromiso ciudadano. Como lo que entra en Internet es muy difícil que desaparezca, hay que sensibilizar al y a la menor en una actitud de cautela y precaución, que valore y enfatice su personalidad, su intimidad e imagen. Todos los elementos físicos y psicológicos, emotivos, cognitivos y conductuales sirven para conformar la complejidad inherente a cada persona. Por esta razón, hasta que pueda asumir de adulto o adulta sus decisiones con mayor libertad y conocimiento, el o la menor debe proteger sus elementos constitutivos para no exponerlos en el laberinto sin salida de la Red.

LUIS FRAGA POMBO

Profesional independente que, tras unha longa traxectoria vinculada aos medios de comunicación, centra a súa actividade na comunicación empresarial e na docencia en comunicación e xornalismo.

Licenciado en Xeografía e Historia pola UNED e máster en Investigación Aplicada en Comunicación pola Universidade Rei Juan Carlos, imparte actualmente clases de xornalismo nas universidades Rei Juan Carlos e Nebrija, ademais de en Atresmediaformacion, e de comunicación empresarial na Escola de Organización Industrial (EOI) e na escola de finanzas EF Business School, entre outros centros educativos. É membro fundador de EduMOTIVAcon, órgano creado pola Consellería de Educación da Xunta de Galicia para o fomento do esforzo e o espírito crítico entre os estudantes non universitarios.

Profesional independiente que, tras una larga trayectoria vinculada a los medios de comunicación, centra su actividad en la comunicación empresarial y en la docencia en comunicación y periodismo.

Licenciado en Geografía e Historia por la UNED y máster en Investigación Aplicada en Comunicación por la Universidad Rey Juan Carlos, imparte actualmente clases de periodismo en las universidades Rey Juan Carlos y Nebrija, además de en Atresmediaformacion, y de comunicación empresarial en la Escuela de Organización Industrial (EOI) y en la escuela de finanzas EF Business School, entre otros centros educativos. Es miembro fundador de EduMOTIVAcon, órgano creado por la Consellería de Educación de la Xunta de Galicia para el fomento del esfuerzo y el espíritu crítico entre los estudiantes no universitarios.

Por que Facebook/Twitter/ Instagram/Google... son gratuítos?

Son gratuítos... daquela maneira. Quero dicir que si estamos "a pagar" dalgún xeito o uso que facemos destas redes sociais. Cando eu me subscribo a Facebook ou a Twitter estou a regalar información persoal ás persoas propietarias destas empresas. Esa información faise máis refinada, más completa, cando eu, por exemplo, dou un "gústame" no Facebook, sigo determinadas persoas en Twitter ou fago unhas buscas en Google. Aí é cando traballan os algoritmos, que fan que eu empece a recibir como resposta suxestións para seguir a persoas cun perfil semellante ás que xa sigo e, o máis destacable, publicidade segundo o meu propio perfil, segundo os gustos mostrados na miña actividade na Rede. E iso ten moito valor. É gratis, vale, porque non pagamos, pero estamos a ceder gratuitamente información que si ten moito valor.

Que é un/unha *prosumidor/a*? Por que hai que aprender a xestionar a nosa actuación como *prosumidores/as*?

A figura do *prosumidor* está moi relacionada coa resposta á pregunta anterior. As marcas divídennos a nós, as persoas

¿Por qué Facebook/Twitter/ Instagram/Google... son gratuitos?

Son gratuitos... de aquella manera. Quiero decir que sí estamos "pagando" de alguna manera el uso que hacemos de estas redes sociales. Cuando yo me suscribo a Facebook o a Twitter estoy regalando información personal a las personas propietarias de estas empresas. Esa información se hace más exquisita, más completa, cuando yo, por ejemplo, doy un "me gusta" en el Facebook, sigo a determinadas personas en Twitter o hago unas búsquedas en Google. Ahí es cuando trabajan los algoritmos, que hacen que yo empiece a recibir como respuesta sugerencias para seguir a personas con un perfil semejante a las que ya sigo y, lo más destacable, publicidad según mi propio perfil, según mis gustos mostrados en mi actividad en la Red. Y eso tiene mucho valor. Es gratis, vale, porque no pagamos, pero estamos cediendo gratuitamente información que sí tiene mucho valor.

¿Qué es un/a *prosumidor/a*? ¿Por qué hay que aprender a gestionar nuestra actuación como *prosumidores/as*?

La figura del *prosumidor* está muy relacionada con la respuesta a la pregunta an-

consumidoras, en perfís construídos grazas á información que nós, consciente ou inconscientemente, lles regalamos. Divídennos por nivel adquisitivo, idade, sexo, mesmo posición ideolóxica ou orientación sexual. Necesitan facelo así porque quen consome xa non é un ser pasivo fronte a elas. Antes, por exemplo, viamos un anuncio na televisión e nós comprabamos ou non o produto segundo o noso criterio; como moito preguntábamos a un amigo ou amiga ou a algún familiar que facía de *prescritor* ou *prescritora.* Agora ese *prescritor* ou *prescritora* está nas redes sociais. Antes de investir unha boa cantidade de cartos nun produto ou servizo miramos en Internet e buscamos opinións. Hai quen se limita a buscar e hai quen crea contidos, interacciona coas marcas e mesmo participa na creación do produto. Este é o perfil de *prosumidor* e *prosumidora* perfectos.

É malo coñecer xente por Internet?

Coñecer xente é positivo case sempre, xente afín a nós coa que compartir o noso ocio, ou xente moi diferente que nos abra a novas vías de pensamento ou que nos descubra outras actividades. Ás veces, na vida real, damos con xente mala, que fai dano. En Internet pasa o mesmo, pero de xeito diferente. A xente "positiva" pode, por suposto, achegarnos moitas cousas, aínda no caso de que esa relación virtual nunca chegue a ser persoal, pero entendo que é no contacto persoal cando unha relación dá os seus froitos. O risco que asumimos en Internet amplifícase coa xente que quere facernos dano de xeito intencionado. O risco é enorme. Por iso recomendo que, até que unha relación non se "desvirtualice" nunca facilitemos datos ou contidos que, de caeren en malas mans, poidan facer que nos arrepintamos.

Todo o contido publicado en Internet é libre.

Estamos feitos a esa idea que di que, efectivamente, todo o que está na Rede ten que ser gratis. É moi difícil facer ver as cousas doutro xeito. Hai que diferenciar aquí entre o contido gratuíto que as empresas son capaces de monetizar sen que nos deamos conta (como vimos no caso das redes sociais) ou con outro tipo de publicacións que si ofrecen ás persoas usuarias a posibilidade de acceder a un

terior. Las marcas nos dividen a nosotras, las personas consumidoras, en perfiles construidos gracias a la información que nosotros y nosotras, consciente o inconscientemente, les regalamos. Nos dividen por nivel adquisitivo, edad, sexo, incluso posición ideológica u orientación sexual. Necesitan hacerlo así porque quien consume ya no es un ser pasivo frente a ellas. Antes, por ejemplo, veíamos un anuncio en la televisión y comprábamos o no el producto según nuestro criterio, como mucho le preguntábamos a un amigo o amiga o a algún familiar que hacía de *prescriptor.* Ahora ese *prescriptor* o *prescriptora* está en las redes sociales. Antes de invertir una buena cantidad de dinero en un producto o servicio miramos en Internet y buscamos opiniones. Hay quien se limita a buscar y hay quien genera contenidos, interacciona con las marcas e incluso participa en la creación del producto. Este es el perfil de *prosumidor* y *prosumidora* perfectos.

¿Es malo conocer gente por Internet?

Conocer gente es positivo casi siempre, gente afín a nosotros y nosotras con la que compartir nuestro ocio, o gente muy diferente que nos abra nuevas vías de pensamiento o que nos descubra otras actividades. A veces, en la vida real, damos con gente mala, que hace daño. En Internet pasa lo mismo, pero de manera diferente. La gente "positiva" puede, por supuesto, aportarnos muchas cosas, aun en caso de que esa relación virtual nunca llegue a ser personal, pero entiendo que es en el contacto personal cuando una relación da sus frutos. El riesgo que asumimos en Internet se amplifica con la gente que quiere hacernos daño de manera intencionada. El riesgo es enorme. Por eso recomiendo que, hasta que una relación no se "desvirtualice", nunca facilitemos datos o contenidos que, si caen en malas manos, puedan hacer que nos arrepintamos.

Todo el contenido publicado en Internet es libre.

Estamos acostumbrados y acostumbradas a esa idea que dice que, efectivamente, todo lo que está en la Red tiene que ser gratis. Es muy difícil hacer ver las cosas de otro modo. Hay que diferenciar aquí entre el contenido gratuito que las

contido restrinxido polo que hai que pagar. No xornalismo, por exemplo, xorden nos últimos anos varios diarios que ofrecen informacións exclusivas para subscritores e subscritoras ou a fórmula de pagamento por noticia.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Que aproveiten todas as posibilidades que nos ofrece o dixital, que non teñan medo senón respecto, é dicir, que tomen medidas para previr os riscos que supón, que os hai, pero que teñan en conta que unha boa xestión da nosa identidade dixital pode dar os seus froitos. Se desde os primeiros anos lle facemos ver aos máis novos e ás máis novas a necesidade de ir construíndo a nosa identidade, de non publicar nada do que nos poidamos arrepentir, de ir pouco a pouco creando contidos relacionados coas nosas afeccións ou aspiracións profesionais, se facemos iso ben, Internet está chea de oportunidades.

empresas son capaces de monetizar sin que nos demos cuenta (como hemos visto en el caso de las redes sociales) o con otro tipo de publicaciones que sí ofrecen a la persona usuaria la posibilidad de acceder a un contenido restringido por el que hay que pagar. En el periodismo, por ejemplo, surgen en los últimos años varios diarios que ofrecen informaciones exclusivas para suscriptores y suscriptoras o la fórmula de pago por noticia.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Que aprovechen todas las posibilidades que nos ofrece lo digital, que no tengan miedo sino respeto, es decir, que tomen medidas para prevenir los riesgos que supone, que los hay, pero que tengan en cuenta que una buena gestión de nuestra identidad digital puede dar sus frutos. Si desde los primeros años hacemos ver a los y las más jóvenes la necesidad de ir construyendo nuestra identidad, de no publicar nada de lo que nos podamos arrepentir, de ir poco a poco creando contenidos relacionados con nuestras aficiones o aspiraciones profesionales, si hacemos eso bien, Internet está llena de oportunidades.

JAVIER GARCÍA BARREIRO

Orientador escolar. Membro da asociación Convives, da que foi o seu presidente. Participa activamente na formación do profesorado en temas relacionados coa mellora da convivencia escolar. É coautor, entre outras, das publicacións "Mediación na práctica" e "Cibermentores".

Orientador escolar. Miembro de la asociación Convives, de la que fue su presidente. Participa activamente en la formación del profesorado en temas relacionados con la mejora de la convivencia escolar. Es coautor, entre otras, de las publicaciones "Mediación en la práctica" y "Cibermentores".

Que é o *sexting*?

É unha práctica erótica que consiste en compartir fotos ou vídeos íntimos a través de Internet entre dúas ou máis persoas de forma consciente, acordada e transparente. De alguén publicar ou compartir sen permiso contido privado como fotos de espidos ou prácticas eróticas ou de extorsionar para conseguilo, iso non é *sexting* senón actos de inxuria e revelación de segredos, delitos penados pola lei.

Ás veces, por vinganzas, roubos, descoidos etc., os contidos acaban difundíndose na Rede e utilizándose para faltar ao respecto ou ben para chantaxear o ou a menor. Neste último caso denomínase *sextorsión.* En adolescentes pode iniciarse como proba de amor (voluntaria ou porque se lle esixe) ou ben para conseguir que se fixen nel ou nela.

Aínda que resulte fácil ver os riscos, é posible entender o sexting desde un enfoque positivo, como unha práctica erótica máis dentro da intimidade da parella que, pola particularidade de realizarse vía Internet, hai que tomar certas precaucións. De decidires libremente facer *sexting,* confías plenamente na persoa e vives unha relación saudable na que non te apertan para facelo, é importante que:

- Non ensines partes do teu corpo (tatuaxes, marcas, *piercings* etc.) ou da túa casa (pósters, cadros...) que te poidan identificar.
- Penses antes de enviar e avises previamente a quen vaia dirixido. Lembra que podes editar, recortar ou ocultar o contido cantas veces queiras antes de subilo.
- Evites as redes wifi públicas e utilices plataformas que che permitan compartir esa foto ou vídeo da forma máis anónima e segura posible coa persoa ou persoas da túa elección. Utilizar a web IMGUR e enviar a ligazón proporciona-

¿Qué es el sexting?

Es una práctica erótica que consiste en compartir fotos o vídeos íntimos a través de Internet entre dos o más personas de forma consciente, acordada y transparente. Si alguien publica o comparte sin permiso contenido privado como fotos de desnudos o prácticas eróticas o si extorsiona para conseguirlo, eso no es *sexting* sino actos de injuria y revelación de secretos, delitos penados por la ley.

A veces, por venganza, robos, descuidos etc., los contenidos acaban difundiéndose en la Red e utilizándose para faltar al respeto o bien para chantajear al o a la menor. En ese último caso se denomina *sextorsión.* En adolescentes puede iniciarse como prueba de amor (voluntaria o porque se le exige) o bien para conseguir que se fijen en él o en ella. Aunque resulte fácil ver los riesgos, es posible entender el sexting desde un enfoque positivo, como una práctica erótica más dentro de la intimidad de la pareja que, por la particularidad de realizarse vía Internet, hay que tomar ciertas precauciones. Si decides libremente hacer sexting, confías plenamente en la persona y vives una relación sana en la que no te presionan para hacerlo, es importante que:

- No enseñes partes de tu cuerpo (tatuajes, marcas, *piercings* etc.) o de tu casa (póster, cuadros...) que te puedan identificar.
- Pienses antes de enviar y avises previamente a quién vaya dirigido. Recuerda que puedes editar, recortar u ocultar el contenido cuantas veces quieras antes de subirlo.
- Evites las redes wifi públicas y utilices plataformas que te permitan compartir esa foto o vídeo de forma más anónima y segura posible con la persona o personas de tu elección. Utilizar la web IM-

da por correo electrónico pode ser unha opción, porque esta páxina permite subir contido sen ter que rexistrarse e o correo electrónico está protexido pola Lei de Protección de Datos. É boa idea crear un correo electrónico que non vaia asociado a datos persoais reais. As redes sociais e de mensaxes habituais (Instagram, Facebook, WhatsApp... e admitindo certas vantaxes, Snapchat) non son seguras, aínda que che permitan enviar fotos ou vídeos en privado, con tempo limitado e autoborrado.

- Borra do móbil ou computador e da nube as fotos ou vídeos, para evitar que por descoidos ou malas intencións acaben difundíndose.

Por contra, de che chegaren fotos ou vídeos íntimos ás túas redes sociais, evita compartir, retuitear ou darlle a "gústame" se non contas co permiso desa persoa, porque estarías a participar como cómplice dunha mala práctica. Se es vítima, garda as probas, cóntao e denúnciao.

Por que é importante formar cidadáns e cidadás dixitalmente competentes?

Ser cidadán e cidadá formados para un mundo dixital supón, en primeiro lugar, aproveitar ao máximo todas as potencialidades para a comunicación e a relación con outras persoas. O mundo dixital é unha ferramenta para o goce, que nos permite expresar e ampliar as nosas capacidades, intereses e relacións ou atopar unha oportunidade creativa de emprego.

Tamén implica que participemos activa e positivamente na construción como colectivo dunha sociedade máis xusta, na que se proxecten os valores éticos e os dereitos democráticos: cando participamos en plataformas de creación e micro financiamento colectivo na Rede (Indiegogo, Kickstarter...) para levar a cabo os nosos proxectos, ideas e soños; ao utilizar plataformas de acollida libre de peticións de carácter cívico, reformista, social e reivindicativo (Change.org, Verkami);

para cambiar situacións que nos parecen inxustas; ou cando creamos e compartimos vídeos colaborativos, memes, gifs ou mensaxes para contestar as noticias e opinións sexistas, homófobas ou racistas que nos chegan, estamos a actuar e participando na sociedade para preservar os dereitos humanos. Por contra, se permaGUR y enviar el enlace proporcionado por correo electrónico puede ser una opción, porque esta página permite subir contenido sin tener que registrarte y el correo electrónico está protegido por la Ley de Protección de Datos. Es buena idea crear un correo electrónico que no vaya asociado a datos personales reales. Las redes sociales y de mensajería habituales (Instagram, Facebook, WhatsApp... y admitiendo ciertas ventajas, Snapchat) no son seguras, aunque te permitan enviar fotos o vídeos en privado, con tiempo limitado y autoborrado.

- Borra del móvil u ordenador y de la nube las fotos o vídeos, para evitar que por descuidos o malas intenciones acaben difundiéndose.

Por contra, si te llegan fotos o vídeos íntimos a tus redes sociales, evita compartir, retuitear o darle a "me gusta" si no cuentas con el permiso de esa persona, porque estarías participando como cómplice de una mala práctica. Si eres víctima, guarda las pruebas, cuéntalo y denúncialo.

¿Por qué es importante formar ciudadanos y ciudadanas digitalmente competentes?

Ser ciudadano y ciudadana formados para un mundo digital supone, en primer lugar, aprovechar al máximo todas las potencialidades para la comunicación y la relación con otras personas. El mundo digital es una herramienta para el disfrute, que nos permite expresar y ampliar nuestras capacidades, intereses y relaciones o encontrar una oportunidad creativa de empleo.

También implica que participemos activa y positivamente en la construcción como colectivo de una sociedad más justa, en la que se proyecten los valores éticos y los derechos democráticos: cuando participamos en plataformas de creación y micro financiación colectiva en la Red (Indiegogo, Kickstarter...) para llevar a cabo nuestros proyectos, ideas y sueños; al utilizar plataformas de acogida libre de peticiones de carácter cívico, reformista, social y reivindicativo (Change.org, Verkami); para cambiar situaciones que nos parecen injustas; o cuando creamos y compartimos vídeos colaborativos, memes, gifs o mensajes para contestar a las noticias y opiniones sexistas, homófobas

necemos impasibles eses dereitos poden verse ameazados.

Por último, é importante edificar de forma voluntaria e máis consciente a imaxe que proxectamos sobre nós mesmos e nós mesmas na Rede, e os datos que ofrecemos a terceiras persoas, mantendo a nosa identidade dixital resgardada do abuso contra os nosos propios intereses e loitando contra a perda de dereitos fundamentais como a liberdade, a intimidade ou o esquecemento en Internet. Porque Internet veu para quedar.

Como teño que actuar se o meu fillo/a é un/unha ciberacosador/a?

Acepto que a súa conduta é inadecuada e quero axudarlle a cambiar.

Para un mozo ou unha moza adolescente é fácil participar dun ciberacoso, porque cando comparte e realiza comentarios ofensivos non ten diante a vítima, non ve como lle está a facer sentir ou canto feren os comentarios. A aparencia de anonimato fai que se desinhiba, que diga todo o que se lle ocorre sen regularse ou pararse a pensar nas consecuencias. Por outra banda, é probable que tamén actúe en compañía doutros e doutras e queira agradar, quedar ben ou sorprender o seu grupo co seu atrevemento. A ofensa esténdese rapidamente a unha ampla audiencia, case sen darnos conta.

Escoito sen xulgar e pescudo que o levou ou que a levou a actuar así, que papel cumpre ou que emocións satisfai desa maneira (agradar, ser líder, a excitación de facer algo prohibido etc.). Sabendo isto, tento apoialo ou apoiala emocionalmente e acompañalo ou acompañala no proceso de reflexión, ensinándolle a pórse no lugar da outra persoa, a sentir o que sente a persoa acosada e, á vez, a que pense antes de actuar, reflexionando sobre as consecuencias que teñen as súas accións, aínda que non sexa consciente delas.

Busco que concrete compromisos prácticos para cambiar a súa conduta e para reparar o dano causado, tanto a nivel persoal coa persoa agraviada, se fose posible, como cara ao público en liña, de transcender a ofensa.

Pouco importa que non saiba de tecnoloxía. É preciso lembrar que o papel da familia sempre foi o de educar en valores

o racistas que nos llegan, estamos actuando y participando en la

sociedad para preservar los derechos humanos. Por contra, si permanecemos impasibles esos derechos pueden verse amenazados.

Por último, es importante edificar de forma voluntaria y más consciente la imagen que proyectamos sobre nosotros mismos y nosotras mismas en la Red, y los datos que ofrecemos a terceras personas, manteniendo nuestra identidad digital a salvo del abuso contra nuestros propios intereses y luchando contra la pérdida de derechos fundamentales como la libertad, la intimidad o el olvido en Internet. Porque Internet ha venido para quedarse.

¿Cómo tengo que actuar si mi hijo/a es un ciberacosador/a?

Acepto que su conducta es inadecuada y quiero ayudarle a cambiar.

Para un chico o una chica adolescente es fácil participar de un ciberacoso, porque cuando comparte y realiza comentarios ofensivos no tiene delante a la víctima, no ve cómo le está haciendo sentir o cuanto hieren los comentarios. La apariencia de anonimato hace que se desinhiba, que diga todo lo que se le ocurre sin regularse o pararse a pensar en las consecuencias. Por otra parte, es probable que también actúe en compañía de otros y otras y quiera agradar, quedar bien o sorprender con su atrevimiento a su grupo. La ofensa se extiende rápidamente a una amplia audiencia, casi sin darnos cuenta.

Escucho sin juzgar y averiguo qué le ha llevado a actuar así, qué papel cumple o qué emociones satisface de esa manera (agradar, ser líder, la excitación de hacer algo prohibido etc.). Conociendo esto, intento apoyar a esa persona emocionalmente y la acompaño en un proceso de reflexión, enseñándola a ponerse en el lugar del otro, a sentir lo que siente la persona acosada y, a la vez, a que piense antes de actuar, reflexionando sobre las consecuencias que tienen sus acciones, aunque no sea consciente de las mismas.

Busco que concrete compromisos prácticos para cambiar su conducta y para reparar el daño causado, tanto a nivel personal con la persona agraviada, si fuera posible, como hacia el público en línea, si la ofensa ha trascendido.

e o ciberacoso é unha decisión moral que vai en contra dos valores de respecto e dignidade. Non quero que o meu fillo ou a miña filla se guíe porque teme un castigo, senón porque constrúa principios morais universais que rexan as súas decisións. Axúdolle entón a que descubra que principios morais se viron comprometidos e educo para actuar en consecuencia.

Promovo que fagan deporte, que teñan contacto coa natureza e determino en que momentos a tecnoloxía non debe estar presente (como na hora de comer ou na de ir para a cama).

Sei que os mozos e as mozas impulsivos e con baixa asertividade son máis propensos e propensas a participar de malos usos en Internet polo que tentarei educar nesas habilidades de vida.

O efecto de grupo é moi importante en redes e pode facer que calquera situación se nos vaia das mans. Que medidas podemos tomar para evitalo?

A adolescencia é unha etapa de grandes cambios. Sentirse membro dun grupo de amigos e amigas, encaixar ou ser apreciado e apreciada pola aula ten moita importancia.

Nas redes ocorre algo parecido. Imaxinemos que unha moza con liderado fai comentarios ofensivos, xulga ou critica nas súas redes sociais alguén do instituto que lle cae mal, ou ben somete esa persoa a escrutinio nalgunha aplicación para determinar se "está bo ou boa" ou "é guai". Probablemente, algúns axiña a apoien cos seus comentarios, engadan máis ofensas e emoticonos burlóns pola excitación de facer algo prohibido, sorprender co seu atrevemento ou agradar. Será difícil que os demais, a gran maioría, reaccionen na Rede por temor a que despois as burlas se dirixan en contra deles ou por non quedar mal. Resulta fácil entrar neste círculo porque non teñen diante a vítima, non ven como a están a facer sentir. Xunto coa sensación de que ninguén vixía, as ofensas continúan e esténdense rapidamente a unha ampla audiencia, o que causa unha sensación de indefensión e falta de control na vítima.

Responder, oporse, implica resistir a esa presión de grupo, saber dicir que non. Dicir non ao grupo require forxar unha boa

Poco importa que no sepa de tecnología. Recuerdo que el papel de la familia siempre ha sido el de educar en valores y el ciberacoso es una decisión moral que va en contra de los valores de respeto y dignidad. No quiero que mi hijo o hija se guíe porque teme un castigo, sino porque construya principios morales universales que rijan sus decisiones. Le ayudo entonces a que descubra qué principios morales se han visto comprometidos y educo para actuar en consecuencia.

Promuevo que hagan deporte, que tengan contacto con la naturaleza y determino en qué momentos la tecnología no debe estar presente (como a la hora de comer o al irse para cama).

Sé que los chicos y chicas impulsivos y con baja asertividad son más propensos y propensas a participar de malos usos en Internet por lo que intentaré educar en esas habilidades de vida.

El efecto de grupo es muy importante en redes y puede hacer que cualquier situación se nos vaya de las manos. ¿Qué medidas podemos tomar para evitarlo?

La adolescencia es una etapa de grandes cambios. Sentirse miembro de un grupo de amigos y amigas, encajar o ser apreciado y apreciada por la clase tiene mucha importancia.

En redes sucede algo parecido. Imaginemos que una chica con liderazgo hace comentarios ofensivos, juzga o critica en sus redes sociales a alguien del instituto que le cae mal, o bien somete esa persona a escrutinio en alguna aplicación para determinar si "está bueno o buena" o "es gay". Probablemente, algunos la apoyen enseguida con sus comentarios, añadan más ofensas y emoticonos burlones por la excitación de hacer algo prohibido, sorprender con su atrevimiento o agradar. Será difícil que los demás, la gran mayoría, reaccionen en la Red por temor a que luego las burlas se dirijan contra ellos y ellas o por no quedar mal. Resulta fácil entrar en este círculo porque no tienen delante a la víctima, no ven cómo le están haciendo sentir. Junto con la sensación de que nadie les vigila, las ofensas continúan y se extienden rápidamente a una amplia audiencia, causando una sensación de indefensión y falta de control en la víctima.

autoestima, autonomía e autocontrol. O autocontrol, por exemplo, implica interiorizar frases do tipo "Parar a pensar antes de enviar ou comentar", "Retuitear, darlle a "gústame" ou compartir unha mensaxe ofensiva convértete en cómplice" ou "Non fagas nada que non farías ou dirías na vida real".

Dicir non require ter empatía no mundo virtual, traballar as emocións, así como a asertividade, é dicir, aprender a dicir o que cada quen pensa tendo en conta a outra persoa. Dicir que non require que o mozo ou a moza analice as consecuencias ás que o leva ou a leva esa conduta e reforzar o seu propio pensamento diante das presións, de maneira que propoña alternativas. Tamén desenvolver valores éticos, como a honestidade e a coherencia, facéndolle ver as consecuencias de actuar baixo o criterio doutras persoas. Trátase dunha decisión que ten que xustificar moralmente. Pero nada pode xustificar a violencia.

Existen programas específicos como PRIRES, co que os e as educadoras fomentan aspectos de empatía virtual, pensamento consecuencial, autocontrol, comunicación e privacidade.

Hai experiencias na escola (Proxecto EPDlav, equipos de cibermentoría) en que se ensina a crear memes, gifs ou vídeos colaborativos pequenos para que respondan, utilizando a mesma linguaxe 2.0, cando ven que se está a ofender a alguén nas redes sociais. Trátase dun activismo en liña que poden facer individualmente, de se sentiren capaces, como grupo de aula ou ben como marca, como membros dun equipo de cibermentoría no seu centro.

Como na adolescencia é importante pasar tempo cos seus iguais, un bo consello pode ser que invistan tempo na Rede en comunidades virtuais con outros e outras adolescentes cos que compartan intereses (crear música, desenvolver aplicacións etc..) e atopar outra forma de participación positiva en grupo.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Que acompañen os seus fillos e as súas fillas ou o seu alumnado no camiño cara á construción da identidade dixital e desenvolvan neles e nelas as habilidades de

Responder, oponerse, implica resistir a esa presión de grupo, saber decir que no. Decir no al grupo requiere forjarse una buena autoestima, autonomía y autocontrol. El autocontrol, por ejemplo, implica interiorizar frases del tipo "Párate a pensar antes de enviar o comentar", "Retuitear, darle a "me gusta" o compartir un mensaje ofensivo te convierte en cómplice" o "No hagas nada que no harías o dirías en la vida real".

Decir no requiere tener empatía en el mundo virtual, trabajar las emociones, así como la asertividad, es decir, aprender a decir lo que uno piensa teniendo en cuenta a otras personas.

Decir que no requiere que el chico o la chica analice las consecuencias a las que le lleva esa conducta y reforzar su propio pensamiento ante las presiones, de manera que proponga alternativas. También desarrollar valores éticos, como la honestidad y la coherencia, haciéndole ver las consecuencias de actuar bajo criterio de otras personas. Se trata de una decisión que tiene que justificar moralmente. Pero nada puede justificar la violencia.

Existen programas específicos como PRIRES, con el que los y las educadoras fomentan aspectos de empatía virtual, pensamiento consecuencial, autocontrol, comunicación y privacidad.

Hay experiencias en la escuela (Proyecto EPDlav, equipos de cibermentoría) donde se les enseña a crear memes, gifs o pequeños vídeos colaborativos para que respondan, utilizando el mismo lenguaje 2.0, cuando ven que se está ofendiendo a alguien en redes sociales. Se trata de un activismo en línea que pueden hacer individualmente, si se sienten capaces, como grupo de clase o bien como marca, como miembros de un equipo de cibermentoría en su centro.

Como en la adolescencia es importante pasar tiempo con sus iguales, un buen consejo puede ser el que inviertan tiempo en la Red en comunidades virtuales con otros y otras adolescentes con quienes compartan intereses (crear música, desarrollar aplicaciones etc..) encontrando otra forma de participación positiva en grupo.

vida necesarias para que edifiquen unha vida persoal e social saudable.

A OMS definiu cales son aquelas 10 habilidades que actúan en favor da saúde en calquera campo, desde a prevención de drogas ao abuso das tecnoloxías, que a educación na familia e na escola deben procurar desenvolver: a empatía, o autocoñecemento, o manexo das emocións e dos conflitos, a toma de decisións etc. http://habilidadesparalavida.net/habilidades.php

Polo tanto, non é necesario saber moito de tecnoloxía. Os valores fundamentais constrúense na familia nos primeiros anos de vida e é a propia familia e a escola quen ofrece, no seu acompañamento, criterio para que os mozos e as mozas apliquen eses principios morais ao mundo virtual, axudándoos e axudándoas a discriminar as condutas non correctas e as ameazas posibles.

Aprender xuntos da tecnoloxía dando valor á conversación, acompañar sen xulgar de antemán e compartir videoxogos e outras actividades cos fillos e coas fillas de forma que a súa conexión á Internet non sexa desde o inicio unha actividade solitaria, serían consellos na mesma liña.

O deseño de móbiles convida ao consumo pasivo. Ese consumo é normalmente individual e silencioso. Familias e educadores e educadoras deben promover xuntas un uso activo da tecnoloxía, de forma que os xogos e as aplicacións que se elixan favorezan a participación e a creatividade. É necesario formarse, por exemplo, a través de escolas de pais e nais. Un estudo da Universidade de Santiago de Compostela (USC) indica que practicar un deporte federado reduce o risco de caer en malos usos de Internet. Tamén o contacto coa natureza e acordar en familia os momentos en que non debe estar presente a tecnoloxía (na hora de comer, por exemplo, ou non levar o móbil na hora de durmir etc.) serían outros consellos.

Por outra banda, un estudo do DCU Anti-Bullying Center de Dublín ofrece as seguintes recomendacións ás familias relacionadas coa prevención do ciberacoso:

1. Fala e escoita o teu fillo ou a túa filla sobre o seu uso de Internet e das redes sociais.
2. Inviste tempo en conversar sobre o ciberacoso e non temas preguntarlles se estiveron implicados ou implicadas

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Que acompañen a sus hijos e hijas o a su alumnado en su camino hacia la construcción de la identidad digital y desarrollen en ellos y en ellas las habilidades de vida necesarias para que edifiquen una vida personal y social saludable.

La OMS ha definido cuales son aquellas 10 habilidades que actúan en favor de la salud en cualquier campo, desde la prevención de drogas al abuso de las tecnologías, que la educación en la familia y en la escuela deben procurar desarrollar: la empatía, el autoconocimiento, el manejo de las emociones y de los conflictos, la toma de decisiones etc. http://habilidadesparalavida.net/habilidades.php

Por tanto, no es necesario saber mucho de tecnología. Los valores fundamentales se construyen en la familia en los primeros años de vida y es la propia familia y la escuela quien ofrece, al acompañarles, criterio para que los chicos y las chicas apliquen esos principios morales al mundo virtual, ayudándolos y ayudándolas a discriminar las conductas no correctas y las posibles amenazas.

Aprender juntos de la tecnología dando valor a la conversación, acompañar sin juzgar de antemano y compartir videojuegos y otras actividades con los hijos y las hijas de forma que su conexión a Internet no sea desde su inicio una actividad solitaria, serían consejos en la misma línea.

El diseño de móviles invita al consumo pasivo. Ese consumo es normalmente individual y silencioso. Familias y educadores y educadoras deben promover juntas un uso activo de la tecnología, de forma que los juegos y aplicaciones que se elijan favorezcan la participación y la creatividad.

Es necesario formarse, por ejemplo, a través de escuelas de padres y madres. Un estudio de la Universidad de Santiago de Compostela (USC) indica que practicar un deporte federado reduce el riesgo de caer en malos usos de Internet. También el contacto con la naturaleza y acordar en familia los momentos en que no debe estar presente la tecnología (a la hora de comer, por ejemplo, no llevar el móvil a la hora de dormir etc.) serían otros consejos.

Por otra parte, un estudio do DCU Anti-Bullying Center de Dublin ofrece las siguientes recomendaciones a las familias

algunha vez como acosadores ou acosadoras, vítimas ou espectadores ou espectadoras.

3. O exceso de confianza non é bo; supervisa.
4. Dille aos e ás menores que non os culparás de seren vítimas de ciberacoso. Non ameaces con que lles vas quitar o móbil xa que esta é a principal razón pola non lle din ás persoas adultas que están a ser vítimas de ciberacoso.

O profesorado, pola súa banda, está a entender que os conflitos relacionados co uso da tecnoloxía son oportunidades de aprendizaxe e que a mellor maneira de evitar as condutas antisociais é ensinar as prosociais. O profesorado está a formarse para responder a este reto educativo. En Galicia xa hai unha materia específica para 1º e 2º da ESO sobre Identidade Dixital e equipos de cibermentoría nalgúns centros. Son mozos e mozas que dan clases ao alumnado de menor idade sobre usos positivos e riscos de Internet, crean e difunden materiais de concienciación e apoian o alumnado que o está a pasar mal por ser vítimas de malos usos en redes sociais.

Tamén cando o profesorado emprega ferramentas dixitais interesantes para desenvolver proxectos na aula, está a ser un modelo para os seus alumnos e alumnas de usos tecnolóxicos positivos.

Os centros están a optar por formas de dar clase que, á vez que melloran a aprendizaxe, ensinan a traballar colaborativamente, favorecen a empatía e outras habilidades de vida. Doutra banda, os equipos de axuda entre iguais (axuda, mediación escolar, titoría entre iguais, mentoría) ofrecen ao alumnado a oportunidade de ensaiar, con guía adulta, competencias socio-emocionais e morais nun ambiente seguro como é a escola.

Existen moi bos programas de educación emocional e de habilidades sociais, así como outros específicos en identidade dixital como PRIRES ou ConRed, ademais de recursos máis centrados en dar información sobre os riscos (Educalike, Pantallas Amigas etc.).

Capacitar o alumnado en habilidades de vida, acompañalo con criterio para facelo máis consciente da construción da súa identidade dixital e promover un uso activo e creativo da tecnoloxía sería ese con-

relacionadas con la prevención del ciberacoso:

1. Habla y escucha a tu hijo o hija sobre su uso de Internet y las redes sociales.
2. Invierte tiempo en conversar sobre el ciberacoso y no temas preguntarles si estuvieron implicados o implicadas alguna vez como acosadores o acosadoras, víctimas o espectadores o espectadoras.
3. El exceso de confianza no es bueno; supervisa.
4. Dile a los y las menores que no los culparás si son víctimas de ciberacoso. No amenaces con que les quitarás el móvil ya que ésta es la principal razón por la no les dicen a las personas adultas que están siendo víctimas de ciberacoso.

El profesorado, por su parte, está entendiendo que los conflictos relacionados con el uso de la tecnología son oportunidades de aprendizaje y que la mejor manera de evitar las conductas antisociales es enseñar las prosociales.

El profesorado se está formando para responder a este reto educativo. En Galicia ya hay una materia específica para 1º y 2º de la ESO sobre Identidad Digital y equipos de cibermentoría en algunos centros. Son chicos y chicas que dan clase al alumnado de menor edad sobre usos positivos y riesgos de Internet, crean y difunden materiales de concienciación y apoyan al alumnado que lo está pasando mal por ser víctima de malos usos en redes sociales.

También cuando el profesorado emplea herramientas digitales interesantes para desarrollar proyectos en el aula está siendo un modelo para sus alumnos y alumnas de usos tecnológicos positivos.

Los centros están optando por formas de dar clase que, a la vez que mejoran el aprendizaje, enseñan a trabajar colaborativamente, favorecen la empatía y otras habilidades de vida. Por otro lado, los equipos de ayuda entre iguales (ayuda, mediación escolar, tutoría entre iguales, mentoría) ofrecen al alumnado la oportunidad de ensayar, con guía adulta, competencias socioemocionales y morales en un ambiente seguro como es la escuela.

Existen muy buenos programas de educación emocional y de habilidades sociales, así como otros específicos en identidad digital como PRIRES o ConRed, además de recursos más centrados en

sello xeral ás familias e aos educadores e educadoras.

dar información sobre los riesgos (Educalike, Pantallas Amigas etc.).

Capacitar al alumnado en habilidades de vida, acompañarles con criterio para hacerles más conscientes de la construcción de su identidad digital y promover un uso activo y creativo de la tecnología sería ese consejo general a familias y educadores y educadoras.

EDITA DE LORENZO

Profesora do Departamento de Teoría do Sinal e Comunicacións e da Escola de Enxeñaría de Telecomunicación.

Directora da Escola de Enxeñaría de Telecomunicación entre 2009 e 2015.

Directora Xeral de PuntoGal entre 2014 e 2017.

Coordinadora do Máster en Enxeñaría de Telecomunicación dende 2014.

Comisionada do Vigo Tecnolóxico da Universidade de Vigo.

Profesora del Departamento de Teoría de la Señal y Comunicaciones y de la Escuela de Ingeniería de Telecomunicación.

Directora de la Escuela de Ingeniería de Telecomunicación entre 2009 y 2015.

Directora General de PuntoGal entre 2014 y 2017.

Coordinadora del Máster en Ingeniería de Telecomunicación desde 2014.

Comisionada de Vigo Tecnológico de la Universidad de Vigo.

Cales son os riscos de estafa actuais en Internet e como podemos previlos?

Internet é unha rede global, inmensa, na que conviven persoas e entidades moi diversas tanto nas súas capacidades como nos seus obxectivos, polo que é doado atopar sitios, aplicacións... que están a agardar a que algunha persoa sen o coidado ou a experiencia precisa sexa enganada.

Só as páxinas, contidos, produtos que veñen dunha entidade fiable o son. Todo o demais pode ter moi variada situación tanto en aspectos legais como éticos. Debemos desenvolver un especial sentido crítico e aprender a asegurarnos de que o que alí aparece vén dunha fonte fiable, tanto se son contidos e consellos como se son promesas de premios e agasallos.

Da mesma maneira que non confiaríamos para comprar ou para crer en calquera persoa descoñecida coa que nos cruzásemos nunha praza ateigada de xente, tampouco o debemos facer con calquera sitio web, mensaxe electrónica ou anuncio que vexamos na praza pública de Internet.

¿Cuáles son los riesgos de estafa actuales en Internet y cómo podemos prevenirlos?

Internet es una red global, inmensa, en la que conviven personas y entidades muy diversas tanto en sus capacidades como en sus objetivos, por lo que es fácil encontrar sitios, aplicaciones... que están esperando a que alguna persona sin el cuidado o la experiencia necesaria sea engañada.

Solo las páginas, contenidos, productos que vienen de una entidad fiable lo son. Todo lo demás puede tener muy variada situación tanto en aspectos legales como éticos. Debemos desarrollar un especial sentido crítico y aprender a asegurarnos de que lo que allí aparece viene de una fuente fiable, tanto que sean contenidos, consejos, o promesas de premios y regalos.

Igual que no confiaríamos al comprar o al creer a cualquier desconocido o desconocida con quien nos cruzásemos en una plaza abarrotada de gente, tampoco lo debemos hacer con cualquier web, mensaje electrónico o anuncio que veamos en la plaza pública de Internet.

Como podemos saber se unha páxina web ou servizo é seguro?

Habería que comprobar que é unha entidade, empresa ou organización na que confiamos e coñecemos. Ademais que os sistemas de verificación, as sinaturas e as referencias, de seren contidos, ou os sistemas de entrega e devolución, de seren compras, por exemplo, son seguras e están certificadas por entidades para tal. E tamén coidar que información privada ou

¿Cómo podemos saber si una página web o servicio es seguro?

Habría que comprobar que es una entidad, empresa u organización en la que confiamos y conocemos. Además, que los sistemas de verificación, las firmas y las referencias, si son contenidos, o los sistemas de entrega y devolución, si son compras, por ejemplo, son seguras y están certificadas por entidades para tal. Y también cuidar qué información privada

persoal estamos a enviar e como o facemos para asegurarnos que non pasa a ser pública e da súa propiedade.

Que é o *phishing*?

Coñécese así unha forma de roubar datos privados mediante mensaxes enganosas que aparentan vir dun banco ou entidade en que confiamos. Desde aí lévannos a unha páxina web similar á real da entidade e na que, ao entrar co noso código e chave, damos información que pode ser utilizada para suplantar a nosa identidade.

Cal é a diferenza entre un *hacker* e un *cracker*?

En xeral chamamos *hacker* a unha persoa experta en redes e/ou servizos informáticos. Un *cracker* sería aquela persoa que usa os seus coñecementos informáticos para causar dano, roubar, atacar... redes de xeito ilegal.

Son seguras as wifi públicas?

As redes wifi públicas son sitios comúns, de acceso libre, polo que todas as persoas que están á vez na Rede deixan alí datos que poden ser utilizados á vez ou posteriormente por quen controle ou entre nesa Rede.

Non son seguras como as privadas e polo tanto deberíamos aumentar as nosas precaucións cando as utilizamos e só facelo para actividades nas que non nos importa "sermos vistos".

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

A identidade dixital é a imaxe que outras persoas teñen de nós en Internet. Todo o que deixamos que esas persoas coñezan de nós.

Internet é unha praza pública na que todos e todas nos amosamos coa nosa presenza en redes sociais, tanto con datos reais como con fotos, opinións, referencias... tal e como decidimos facelo. O xeito de vestir, de aparecer, de falar, de comportarnos vai ser visto por moita xente que non coñecemos e que non sabemos en que momento ou forma utilizarán a información que nós lles amosemos xa que estamos nun escaparate que calque-

o personal estamos enviando y cómo lo hacemos para asegurarnos que no pasa a ser pública y de su propiedad.

¿Qué es el *phishing*?

Se conoce así una forma de robar datos privados mediante mensajes trucados que aparentan venir de un banco o entidad en la que confiamos. Desde ahí nos llevan a una página web similar a la real de la entidad y que al entrar con nuestro código y llave les damos información que puede ser utilizada para suplantar nuestra identidad.

¿Cuál es la diferencia entre un *hacker* y un *cracker*?

En general llamamos hacker a una persona experta en redes y/o servicios informáticos. Un cracker sería aquella persona que usa sus conocimientos informáticos para causar daño, robar, atacar... redes de manera ilegal.

¿Son seguras las wifi públicas?

Las redes wifi públicas son sitios comunes, de acceso libre, por lo que todas las personas que están a la vez en la Red dejan allí datos que pueden ser utilizados a la vez o posteriormente por quien controle o entre en esa Red.

No son seguras como las personales y por lo tanto deberíamos aumentar nuestras precauciones cuando las utilizamos y solo hacerlo para actividades en las que no nos importa "ser vistos".

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

La identidad digital es la imagen que otras personas tienen de nosotros en Internet. Todo lo que dejamos que esas personas conozcan de nosotros.

Internet es una plaza pública en la que todos y todas nos mostramos con nuestra presencia en redes sociales, tanto con datos reales como fotos, opiniones, referencias... tal y como decidimos hacerlo. La manera de vestir, de aparecer, de hablar, de comportarnos va a ser vista por mucha gente que no conocemos y que no sabemos en que momento o forma utilizarán la información que les mostramos ya que estamos en un escaparate que cualquiera

ra pode ver mentres o facemos ou moito tempo despois.

Todo o que temos exposto en redes sociais, páxinas web... vai quedar nas mans dos seus donos e donas (que poden facer o que queiran se nós lles damos ese dereito ou autorizamos) e tamén vai ser vista por quen lle deamos permiso para velo. E esta información pode quedar por anos e chegar a persoas moi distintas coas que no futuro pode que nos atopemos en relacións persoais, sociais, laborais... de calquera tipo.

Debemos ser conscientes e preguntarnos: que queremos que vexan e saiban de nós? Estas persoas van ver o que nós deixemos á súa disposición, o que nós decidamos que é a nosa identidade dixital...

puede ver mientras lo hacemos o mucho tiempo después.

Todo lo que hemos expuesto en redes sociales, páginas web... va a quedar en manos de sus dueños y dueñas (que pueden hacer lo que quieran si les damos ese derecho o autorizamos) y también va a ser vista por quien le demos permiso para verlo. Y esta información puede quedar por años y llegar a personas muy distintas con las que en el futuro puede que nos encontremos en relaciones personales, sociales, laborales... de cualquier tipo.

Debemos ser conscientes y preguntarnos: ¿qué queremos que vean y sepan de nosotros y nosotras? Estas personas van a ver lo que nosotros y nosotras dejemos a su disposición, lo que decidamos que es nuestra identidad digital...

OLEGARIA MOSQUEDA BUENO

Psicóloga. Vogal da Xunta Directiva do Colexio oficial de Psicoloxía de Galicia.

Orientadora do IES Santa Irene de Vigo, desde 1989 ata a actualidade.

Especialista en Apoio Psicopedagóxico e Orientación Educativa.

Educadora en Internado Universidade Laboral de Vigo durante 11 anos.

Psicóloga desde o 2005 do Grupo Intervención Psicolóxica Catástrofes e Emerxencias (GIPCE).

Psicóloga. Vocal de la Junta Directiva del Colegio oficial de Psicología de Galicia.

Orientadora del IES Santa Irene de Vigo, desde 1989 hasta la actualidad.

Especialista en Apoyo Psicopedagógico y Orientación Educativa.

Educadora en Internado Universidad Laboral de Vigo durante 11 años.

Psicóloga desde 2005 del Grupo Intervención Psicológica Catástrofes y Emergencias (GIPCE).

Que uso dos dispositivos electrónicos ou de Internet se considera excesivo ou problemático?

Será excesivo todo aquel uso que atente contra a identidade, intimidade e integridade do ou da menor. Debemos protexer a súa inocencia e descoñecemento dos perigos que supoñen as tecnoloxías.

Por iso unha boa información e un control do tempo de uso e utilización de contidos é fundamental.

En canto aos contidos hai un exceso de violencia en vídeos e xogos que reforzan as condutas violentas e agresivas, antisociais, racistas, sexistas...

A hipersexualización en series, debuxos, música e bailes é produto de consumo en idades moi temperás que se difunden sen filtro nin control.

Poderiamos citar como usos problemáticos os seguintes:

- WhatsApp e mensaxes de texto insultantes, difamatorias e/ou ameazantes, con mentiras, desvalorizantes ou intimidatorias.
- Difusión de imaxes e manipulación (vídeos e fotos). Para ridiculizar ou crear unha imaxe falsa por móbil ou Internet.
- Chamadas anónimas ameazantes. Para atemorizar.
- Excluír, illar nas redes sociais: Facebook, Tuenti, WhatsApp, Instagram...
- Roubar o contrasinal, suplantar a identidade, enviar mensaxes agresivas a contactos para que rexeiten a vítima...

¿Qué uso de los dispositivos electrónicos o de Internet se considera excesivo o problemático?

Será excesivo todo aquel uso que atente contra la identidad, intimidad e integridad del o de la menor. Debemos proteger su inocencia y desconocimiento de los peligros que conllevan las tecnologías.

Por eso una buena información y control del tiempo de uso y utilización de contenidos es fundamental.

En cuanto a los contenidos hay un exceso de violencia en vídeos y juegos que refuerzan las conductas violentas y agresivas, antisociales, racistas, sexistas...

La hipersexualización en series, dibujos, música y bailes es producto de consumo en edades muy tempranas que se difunden sin filtro ni control.

Podríamos citar como usos problemáticos los siguientes:

- WhatsApp y mensajes de texto insultantes, difamatorios y/o amenazantes, con mentiras, desvalorizantes o intimidatorios.
- Difusión de imágenes y manipulación (vídeos y fotos). Para ridiculizar o crear una imagen falsa por móvil o Internet.
- Llamadas anónimas amenazantes. Para atemorizar.
- Excluir, aislar en las redes sociales: Facebook, Tuenti, WhatsApp, Instagram...
- Robar la contraseña, suplantar la identidad, enviar mensajes agresivos a contactos para que rechacen a la víctima...
- *Sexting* o divulgación de fotos en ropa interior o sin ella, comprometidas por su carácter sexual.

- *Sexting* ou divulgación de fotos en roupa interior ou sen ela, comprometidas polo seu carácter sexual.
- *Grooming:* captación de nenos e nenas por persoas adultas que se fan pasar por menores para gañar confianza, conseguir fotos ou vídeos, ameazando e chantaxeando despois, chegando ao abuso sexual.

Como teño que actuar se o meu fillo/a é un/unha ciberacosador/a?

Custa asumir que un fillo ou unha filla é un agresor ou agresora a través das redes, pero non é cousa de menores e o seu futuro está en xogo (posibles consecuencias penais).

A actitude da familia debe ser sempre firme, asumindo a situación, deixando claro que a familia non tolera nin xustifica este tipo de condutas.

Hai que falar directamente do que está a pasar e actuar con calma. Investigar por que é un acosador ou unha acosadora.

Non se debe culpar os outros pola conduta do fillo ou filla.

Indagar sobre a súa participación en grupos que actúan impunemente e comunicarlle que debe romper ese tipo de relacións.

Debe reparar os danos, pedir perdón e cambiar a súa actitude.

Ofrecerlle axuda ao seu fillo ou filla para que recoñeza a súa responsabilidade e autoría:

1. Ensinarlle a practicar boas condutas e practicar a empatía: pórse no lugar da outra persoa; aceptar as diferentes Reaccións, Emocións e Sensibilidades dos demais. Eloxiar as súas accións positivas e manter un seguimento.
2. Facerlle ver que esas condutas son daniñas e perigosas tanto para a vítima como para el ou ela. Transmitirlle que ese problema preocupa á familia e que hai que atallalo.
3. Os proxenitores deben ser modelos de conduta prosocial, empatía e non violencia.

Deben ter unha alta aceptación da situación e unha efectiva implicación, así como uns niveis razoables de disciplina, imposición e castigo...

Solicitar asesoramento ao Equipo Directivo e ao Departamento de Orientación do

- *Grooming:* captación de niños y niñas por personas adultas que se hacen pasar por menores para ganar confianza, conseguir fotos o vídeos, amenazando y chantajeando después, llegando al abuso sexual.

¿Cómo tengo que actuar si mi hijo/a es un ciberacosador/a?

Cuesta asumir que un hijo o una hija es un agresor o una agresora a través de las redes, pero no es cosa de menores y su futuro está en juego (posibles consecuencias penales).

La actitud de la familia debe ser siempre firme, asumiendo la situación, dejando claro que la familia no tolera ni justifica este tipo de conductas.

Hay que hablar directamente de lo que está pasando y actuar con calma. Investigar por qué es un acosador o una acosadora.

No se debe culpar a otros por la conducta del hijo o de la hija.

Indagar sobre su participación en grupos que actúan impunemente y comunicarle que debe romper ese tipo de relaciones.

Debe reparar los daños, pedir perdón y cambiar su actitud.

Ofrecer ayuda a su hijo o hija para que reconozca su responsabilidad y autoría.

1. Enseñarle a practicar buenas conductas y practicar la empatía: ponerse en el lugar de otra persona; aceptar las diferentes Reacciones, Emociones y Sensibilidades de los demás. Elogiar sus buenas acciones y mantener un seguimiento.
2. Hacerle ver que esas conductas son dañinas y peligrosas tanto para la víctima como para el o ella. Transmitirle que ese problema preocupa a la familia y que hay que atajarlo.
3. Los progenitores deben ser modelos de conducta prosocial, empatía y no violencia.

Deben tener una alta aceptación de la situación y una efectiva implicación, así como unos niveles razonables de disciplina, imposición y castigo...

Solicitar asesoramiento al Equipo Directivo y Departamento de Orientación del centro educativo.

Acudir a terapia si fuese necesario para trabajar:

centro educativo.

Acudir a terapia de ser necesario para traballar:

1. A empatía.
2. Regulación emocional: control da ira, impulsividade e frustración.
3. Habilidades sociais. Asertividade e conduta prosocial.
4. Resolución pacífica de conflitos.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Familias: Non é conveniente que comece a utilizarse con idades moi temperás (non antes dos 13 anos), xa que diminúe a súa concentración e atención, pode provocar illamento, trastornos de conduta, alteración e diminución do sono, roubando tempo de dedicación ao estudo ou a outras actividades recreativas máis creativas, saudables e en concordancia coa súa etapa de desenvolvemento físico e intelectual. Deben controlar o uso que os seus fillos e as súas fillas fan das redes e Internet.

Profesorado: Informar dos riscos e perigos que supoñen as redes e limitar o tempo de utilización cunhas normas claras de uso e boa utilización.

1. La empatía.
2. Regulación emocional: control de la ira, impulsividad y frustración.
3. Habilidades sociales. Asertividad y conducta prosocial.
4. Resolución pacífica de conflictos.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Familias: No es conveniente que comience a utilizarse a edades muy tempranas (no antes de los 13 años), ya que disminuye su concentración y atención, puede provocar aislamiento, trastornos de conducta, alteración y disminución del sueño, robando tiempo de dedicación al estudio o a otras actividades recreativas más creativas, saludables y en concordancia con su etapa de desarrollo físico e intelectual. Deben controlar el uso que sus hijos y sus hijas hacen de las redes e Internet.

Profesorado: Informar de los riesgos y peligros que conllevan las redes y limitar el tiempo de utilización con unas normas claras de uso y buena utilización.

JAVIER PEDREIRA "WICHO"

Responsable de informática dos Museos Científicos Coruñeses e un dos creadores de Microsiervos, un dos blogs sobre ciencia e tecnoloxía máis lidos en español. É tamén colaborador habitual de medios de comunicación como El País, a Cadena SER, Muy Interesante e outros, así como da plataforma de divulgación científica Naukas.

Responsable de informática de los Museos Científicos Coruñeses y uno de los creadores de Microsiervos, uno de los blogs sobre ciencia y tecnología más leídos en español. Es también colaborador habitual de medios de comunicación como El País, la Cadena SER, Muy Interesante y otros, así como de la plataforma de divulgación científica Naukas.

Que consellos de seguridade en Internet deberían seguir todas as familias?

Hai un básico e moi sinxelo que pode axudar a evitar moitos desgustos como é instalar un antivirus no dispositivo co que se accede a Internet e mantelo actualizado. Isto evitará perdas e roubos de datos, a activación en remoto da webcam, e cousas polo estilo.

Pero é moito máis importante educar aos rapaces en cuestións básicas coma que os contrasinais teñen que ser seguros, mesturando letras en minúsculas e maiúsculas con números e símbolos e que estas, como o cepillo de dentes, non se comparten.

E, sobre todo, estar ao seu lado cando empecen a utilizar Internet para ver como configuran as opcións de privacidade das contas dos servizos nos que se dan de alta e asegurarnos de que nos deixan seguilos aínda que non vaiamos interactuar con eles a través das súas contas en redes sociais se eles non o queren.

Este estar ao seu lado tamén ten que ser físico ao principio, de tal forma que usen o computador, tablet ou móbil nun espazo común da casa, non para espialos senón para que saiban que se teñen alguna dúbida estamos ao seu carón.

E tamén é fundamental que desde un primeiro momento establezamos unha especie de acordo en canto ao tempo que lle poden dedicar ao smartphone ou ao computador ao día e que haxa espazos nos que este quede de lado, como pode ser a mesa da cociña á hora para comer e cear. Querer chegar a un acordo así cando os rapaces están acostumados e estar conectados acotío e en todo momento é practicamente imposible.

¿Qué consejos de seguridad en Internet deberían seguir todas las familias?

Hay uno básico y muy sencillo que puede ayudar a evitar muchos disgustos como es instalar un antivirus en el dispositivo con el que se accede a internet y mantenerlo actualizado. Esto evitará pérdidas y robos de datos, la activación en remoto de la webcam, y cosas por el estilo.

Pero es mucho más importante educar a los chavales y chavalas en cuestiones básicas como que las contraseñas tienen que ser seguras, mezclando letras en minúsculas y mayúsculas con números y símbolos y que estas, como el cepillo de dientes, no se comparten.

Y, sobre todo, estar a su lado cuando empiecen a utilizar internet para ver como configuran las opciones de privacidad de las cuentas de los servicios en los que se dan de alta y asegurarnos de que nos dejan seguirlos y seguirlas, aunque no vayamos a interactuar con ellos o ellas a través de sus cuentas en redes sociales si no quieren.

Este estar a su lado también tiene que ser físico al principio, de tal forma que usen el ordenador, tableta o móvil en un espacio común de la casa, no para espiar sino para que sepan que si tienen alguna duda estamos a su lado.

Y también es fundamental que desde un primer momento establezcamos una especie de acuerdo en cuanto al tiempo que le pueden dedicar al smartphone o al ordenador al día y que haya espacios en los que este quede de lado, como puede ser la mesa de la cocina a la hora de comer y cenar. Querer llegar a un acuerdo así cuando tienen la costumbre de estar conectados y conectadas a todas horas y en todo momento es prácticamente imposible.

A partir de que idade é recomendable que os/as menores teñan móbil?

Esta é a pregunta do millón, e facendo gala do meu galeguismo direi que depende.

Por lei non poden estar en redes sociais antes dos 14 anos, pero todos sabemos que desde moito antes hai unha presión, aínda que só sexa pola súa contorna, para ter móbil, e que cada vez máis, é o agasallo estrela da primeira comuñón.

E aquí cada familia e cada menor son un mundo, así que son os seus pais ou titores legais os que deben decidir en que momento se lle dá un móbil ao menor.

Non hai unha cifra máxica que sirva para todos; de feito dentro da mesma familia pode haber respostas distintas a esta pregunta segundo o grao de madurez do menor.

O que é extremadamente importante é estar ao seu lado sexa cal for a idade á que empeza a usar o móbil.

E optar por non darllo ata que cumpra 18 anos e poida compralo él tampouco parece unha opción razoable, xa que non dispor dun móbil exclúeo da súa contorna.

De sermos coidadosos/as é posible controlar o que subimos a Internet e retiralo cando queiramos.

Esta pregunta ten unha resposta moi sinxela: non.

Por moi coidadosos que sexamos á hora de subir contidos a Internet e apliquemos filtros para restrinxir quen pode velo ou non sempre estamos expostos a que alguén faga unha captura de pantalla e que comparta eses contidos aínda en contra da nosa vontade.

Tamén se pode producir un fallo de seguridade que expoña os nosos datos ou que alguén se faga co contrasinal da nosa conta e con eles e os distribúa por aí.

Ademais, aínda que nunca lemos os termos de uso dos servizos nos que nos damos de alta, en moitos estamos a aceptar que os nosos datos poden estar nos seus servidores durante algún tempo aínda se decidimos borralos.

Así que o mellor é asumir que en canto subimos calquera cousa a Internet perdemos o control sobre esta, por moi coidadosos que sexamos.

¿A partir de qué edad es recomendable que los/las menores tengan móvil?

Esta es la pregunta del millón, y haciendo gala de mi galleguismo diré que depende.

Por ley no pueden estar en redes sociales antes de los 14 años, pero todos y todas sabemos que desde mucho antes hay una presión, aunque sólo sea por su entorno, para tener móvil, y que cada vez más, es el regalo estrella de la primera comunión.

Y aquí cada familia y cada menor son un mundo, así que son sus padres, madres o la tutela legal quienes deben decidir en qué momento se le da un móvil al menor o a la menor.

No hay una cifra mágica que sirva para todo el mundo; de hecho, dentro de la misma familia puede haber respuestas distintas a esta pregunta según el grado de madurez del menor o de la menor.

Lo que es extremadamente importante es estar a su lado sea cual sea la edad a la que empieza a usar el móvil.

Y optar por no dárselo hasta que cumpla 18 años y se lo compre él o ella tampoco parece una opción razonable, ya que no disponer de móvil puede ser excluyente de su entorno.

Si somos personas cuidadosas es posible controlar lo que subimos a Internet y retirarlo cuando queramos.

Esta pregunta tiene una respuesta muy sencilla: no.

Por mucho cuidado que tengamos a la hora de subir contenidos a internet y apliquemos filtros para restringir quien puede verlo o no siempre nos exponemos a que alguien haga una captura de pantalla y que comparta esos contenidos aún en contra de nuestra voluntad.

También se puede producir un fallo de seguridad que exponga nuestros datos o que alguien se haga con la contraseña de nuestra cuenta y se haga con ellos y los distribuya por ahí.

Además, aunque nunca nos leemos los términos de uso de los servicios en los que nos damos de alta, en muchos estamos aceptando que nuestros datos pueden estar en sus servidores durante algún tiempo aún si decidimos borrarlos.

Con iso non quero dicir que non subamos nada a Internet, por suposto, só que hai que ser consciente de a que nos expomos.

É bo que as rapazas e os rapaces teñan o seu propio ordenador? De teren ordenador, que consellos deberíamos seguir como pais e nais?

Poida que non necesariamente o seu propio computador, pero desde logo si unha conta nalgún computador que haxa na casa para poder usalo ao seu gusto. No mundo no que van vivir os nosos fillos e alumnos o computador e Internet son ferramentas que van usar en todos os aspectos da súa vida, así que canto antes o incorporen nelas como unha ferramenta transversal, mellor.

Ademais, cada vez máis as empresas demandan, xunto aos idiomas, que calquera que solicite traballo sexa competente no uso de ferramentas como o correo electrónico ou contornas de traballo colaborativo como *Google Docs.* E son un tipo de competencias que dificilmente se adquiren mediante un móbil ou unha tablet porque «protexen» demasiado ao usuario de como funciona todo por baixo, así que darlles acceso a un computador é unha forma de ir traballando na súa futura empregabilidade.

Iso si, sobre todo ao principio, é moi importante que o computador estea nun espazo común da casa, para que os rapaces saiban que estamos aí e que non poden facer o indio co computador de calquera xeito; hai que darlles formación en valores no uso do computador igual que o facemos no mundo real. Crer que activando os controis parentais non temos máis nada que facer é un grave erro: estes son limitados, é fácil que se equivoquen e filtren o que non deben e ao revés, e é fácil que os rapaces terminen saltándoos ou usando un computador que non os teña.

É importante tamén instalar un antivirus e mantelo actualizado para evitar perdas e roubos de datos e cousas como que alguén poida acceder en remoto á cámara do computador se a ten.

As nenas e os nenos que naceron despois da popularización dos ordenadores, son nativas e nativos dixitais?

Outra pregunta con resposta fácil: non, en absoluto, non son nativos dixitais.

Así que lo mejor es asumir que en cuanto subimos cualquier cosa a internet perdemos el control sobre esta, por mucho cuidado que tengamos.

Con ello no quiero decir que no subamos nada a internet, por supuesto, sólo que hay que ser consciente de a qué nos exponemos.

¿Es bueno que los/las jóvenes tengan su propio ordenador? Si tienen ordenador, ¿qué consejos deberíamos seguir como padres y madres?

Puede que no necesariamente su propio ordenador, pero desde luego sí una cuenta en algún ordenador que haya en casa para poder usarlo a su gusto. En el mundo en el que van a vivir nuestros hijos e hijas y alumnado, el ordenador e internet son herramientas que van a usar en todos los aspectos de su vida, así que cuanto antes lo incorporen como una herramienta transversal en ellas, mejor.

Además, cada vez más las empresas demandan, junto a los idiomas, que cualquiera que solicite trabajo sea competente en el uso de herramientas como el correo electrónico o entornos de trabajo colaborativo como *Google Docs.* Y son un tipo de competencias que difícilmente se adquieren mediante un móvil o una tableta porque «protegen» demasiado a la persona usuaria de cómo funciona todo por debajo, así que darles acceso a un ordenador es una forma de ir trabajando en su futura empleabilidad.

Eso sí, sobre todo al principio, es muy importante que el ordenador esté en un espacio común de la casa, para que los chavales y chavalas sepan que estamos ahí y que no pueden hacer el indio con el ordenador de cualquier manera; hay que darles formación en valores en el uso del ordenador igual que lo hacemos en el mundo real. Creer que activando los controles parentales no tenemos nada más que hacer es un grave error: éstos son limitados, es fácil que se equivoquen y filtren lo que no deben y al revés, y es fácil que los chavales y chavalas terminen saltándoselos o usando un ordenador que no los tenga.

Es importante también instalar un antivirus y mantenerlo actualizado para evitar pérdidas y robos de datos y cosas como que alguien pueda acceder en remoto a la cámara del ordenador si la tiene.

Aínda que é certo que non lle teñen o respecto –ou quizais medo nalgúns casos– que os que medramos sen ese tipo de acceso a computadores e internet, tamén o é que non é verdade que saiban facer un uso correcto desas ferramentas.

Seica por vivir nunha casa na que hai armarios non lles hai que explicar que deben usalos e ter os seus cuartos en orde? Ou por nacer en familias que seguramente teñen automóbil xa non temos que sacar o carné de conducir?

Pois cos supostos nativos dixitais pasa un pouco o mesmo. Basta con rascar un pouco por baixo da superficie para ver que en realidade non todos os mozos son eses supostos «nativos dixitais», nin moito menos.

Moitos deles se os sacas de Instagram, Snapchat ou Youtube ou dos programas que utilizan para descargarse música e películas, son tan zoupóns como o que máis. Tampouco teñen nin idea dos seus dereitos e deberes nesta era dixital.

E iso sen poñernos a falar da súa falta de criterio á hora de buscar información en internet. Vanse a Google e aínda que poida que non pulsen o botón «Vou ter sorte» quedan co primeiro resultado que atopan e non se preguntan por que está ese resultado aí, quen o puxo e con que intencións, e nin tan sequera se preocupan de buscar outro punto de vista, a pesar de que o teñen máis fácil que nunca na historia.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Que tomen conciencia de que os nosos fillos e alumnos necesitan saber que os mesmos valores que lles aprendemos no mundo real teñen que aplicalos na súa vida en liña, que o que fan en Internet ten consecuencias de cara á súa imaxe persoal, o que á vez pode influír nas súas posibilidades de conseguir un traballo, e que tamén pode ter consecuencias legais. Así que non vale con mirar para outro lado coa desculpa de que son nativos dixitais; temos que estar ao seu carón nesta aprendizaxe, igual que o estamos, ou deberíamos estar, no resto das aprendizaxes da súa vida.

Los niños y niñas que nacieron después de la popularización de los ordenadores, ¿son nativos y nativas digitales?

Otra pregunta con respuesta fácil: no, en absoluto, no son nativos y nativas digitales.

Si bien es cierto que no le tienen el respeto –o quizás miedo en algunos casos– de las personas que hemos crecido sin ese tipo de acceso a ordenadores e internet, también lo es que no es verdad que sepan hacer un uso correcto de esas herramientas.

¿Acaso por vivir en una casa en la que hay armarios no les tenemos que explicar que deben usarlos y tener sus cuartos en orden? ¿O por nacer en familias que seguramente tienen automóvil ya no tenemos que sacar el carnet de conducir? Pues con los supuestos nativos y nativas digitales pasa un poco lo mismo. Basta con rascar un poco por debajo de la superficie para ver que en realidad no toda la juventud es esa supuesta «nativa digital», ni mucho menos.

Mucha de esa juventud, si la sacas de Instagram, Snapchat o YouTube o de los programas que utiliza para descargarse música y películas, es tan patosa como la que más. Tampoco tienen ni idea de sus derechos y deberes en esta era digital.

Y eso sin ponernos a hablar de su falta de criterio a la hora de buscar información en internet. Se van a Google y aunque puede que no pulsen el botón «Voy a tener suerte» se quedan con el primer resultado que encuentran y no se preguntan porqué está ese resultado ahí, quién lo ha puesto y con qué intenciones, y tan siquiera se preocupan de buscar otro punto de vista, a pesar de que lo tienen más fácil que nunca en la historia.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Que tomen conciencia de que nuestros hijos e hijas y alumnado necesitan saber que los mismos valores que les enseñamos en el mundo real tienen que aplicarlos en su vida on line, que lo que hacen en internet tiene consecuencias de cara a su imagen personal, lo que a la vez puede influir en sus posibilidades de conseguir un trabajo, y que también puede tener consecuencias legales. Así que no vale con

mirar para otro lado con la disculpa de que son nativos y nativas digitales; tenemos que estar a su lado en este aprendizaje, igual que lo estamos, o deberíamos estar, en el resto de los aprendizajes de su vida.

ANTONIO RIAL BOUBETA

Doutor en Psicoloxía Social e Profesor Titular da Universidade de Santiago de Compostela. Director técnico da Unidade de Psicoloxía do Consumidor e Usuario e experto en metodoloxía de investigación en ciencias sociais e da saúde. Autor de máis dun centenar de artigos en revistas científicas nacionais e internacionais, director de 15 teses doutorais e responsable de diferentes proxectos de investigación no ámbito dos adolescentes, desde o uso problemático de Internet, as redes sociais e as TIC, o *cyberbullying* ou o consumo de alcol e outras drogas. É autor tamén do libro "Adolescentes e Novas Tecnoloxías: unha responsabilidade compartida" e colaborador habitual de diferentes medios de comunicación.

Doctor en Psicología Social y Profesor Titular de la Universidad de Santiago de Compostela. Director técnico de la Unidad de Psicología del Consumidor y Usuario y experto en metodología de investigación en ciencias sociales y de la salud. Autor de más de un centenar de artículos en revistas científicas nacionales e internacionales, director de 15 tesis doctorales y responsable de diferentes proyectos de investigación en el ámbito de los adolescentes, desde el uso problemático de Internet, las redes sociales y las TIC, el *cyberbullying* o el consumo de alcohol y otras drogas. Es autor también del libro "Adolescentes y Nuevas Tecnologías: una responsabilidad compartida" y colaborador habitual de diferentes medios de comunicación.

A que idade pode un/unha menor ter WhatsApp/Line/Telegram?

É un feito constatable que o acceso ás novas tecnoloxías se está a producir cada vez a idades máis temperás. Actualmente o acceso ao primeiro móbil con datos prodúcese por termo medio aos 11 anos xustos, e o uso de tabletas, videoconsolas e outros dispositivos tecnolóxicos aínda moito antes. Iso obviamente ten as súas vantaxes, pero tamén os seus perigos, como unha hiperestimulación continuada e un deterioro das rutinas dos nenos e das nenas e do seu estilo de vida, que non sempre é saudable. Semella evidente pensar na conveniencia de retardar o acceso ao primeiro móbil, segundo persoas expertas non antes dos 12 anos. Pero é preciso deixar claro que non é tanto cuestión de idade mínima de acceso, senón de educación, do que teñamos feito como nais e pais (e como educadores e educadoras) antes e do que imos facer despois.

A partir de que idade é conveniente que os nenos e as nenas teñan WhatsApp ou teñan móbil? Pregúntome se alguén se cuestiona a partir de que idade poden saír cos seus amigos e amigas, beber a súa primeira cervexa ou experimentar co primeiro "bico con lingua", como se se tratase dunha fronteira exacta capaz de delimitar o que pode ou non pode facerse de xeito saudable. *Cada casa é un mundo.* Por iso o importante en cada

¿A qué edad puede un/a menor tener WhatsApp/Line/Telegram?

Es un hecho constatable que cada vez el acceso a las nuevas tecnologías se está produciendo a edades más tempraneras. Actualmente el acceso al primer móvil con datos se produce por término medio a los 11 años justos, y el uso de tabletas, videoconsolas y otros dispositivos tecnológicos aún mucho antes. Eso obviamente tiene sus ventajas, pero también sus peligros, como una hiperestimulación continuada y un deterioro de las rutinas de los niños y las niñas y de su estilo de vida, que no siempre es saludable. Parece evidente pensar en la conveniencia de atrasar el acceso al primer móvil, según personas expertas no antes de los 12 años. Pero es necesario dejar claro que no es tanto cuestión de edad mínima de acceso, sino de educación, de lo que hayamos hecho como madres y padres (y como educadores y educadoras) antes y de lo que vamos a hacer después.

¿A partir de qué edad es conveniente que los niños y las niñas tengan WhatsApp o tengan móvil? Me pregunto si alguien se cuestiona a partir de qué edad pueden salir con sus amigos y amigas, beber su primera cerveza o experimentar con el primer "beso con lengua", como si se tratara de una frontera exacta capaz de delimitar lo que puede o no puede hacerse de manera saludable. *Cada casa es*

un deses casos non é a idade concreta a golpe de calendario, senón que fixemos antes dese momento e que pensamos facer a continuación, que normas e pautas imos establecer. Nais e pais debemos ser moi conscientes de que detrás de todos estes novos dispositivos e aplicacións hai un verdadeiro risco, non só polos contidos aos que os nosos fillos e as nosas fillas poden acceder e a cantidade de leas nas que se poden meter, senón sobre todo no que deixan de facer e no tipo de persoas en que se poden chegar a converter. Algo tan aparentemente inocuo como un teléfono móbil ten demostrado unha capacidade enorme de influír nas nosas vidas, de modificar a rutina e o estilo de vida de grandes e pequenos máis alá do que podemos imaxinar... porque ao final acabamos por ser o que facemos cada día, as cousas nas que ocupamos cada minuto e cada hora das nosas vidas.

Que é o *grooming*?

En termos xenéricos poderíase dicir que se trata dun novo xeito de pederastia, vinculada a Internet e ás redes sociais, que está a suscitar cada vez maior preocupación social. Pódese definir como unha serie de prácticas en liña de certas persoas adultas para gañar a confianza dun ou dunha menor finxindo empatía, cariño... con fins de satisfacción sexual; persoas adultas, por exemplo, que crean un perfil falso nunha rede social ou nunha aplicación de videoxogos en liña, facéndose pasar por un ou unha menor, coa intención manifesta de gañar a súa confianza nun breve lapso de tempo e chegar a ter finalmente un contacto sexual. Esta práctica constitúe un novo tipo delitivo que vén recollido na última reforma do código penal, no artigo 183.

Se ben é difícil contar con datos fiables sobre o volume de casos existentes nas diferentes comunidades e países da nosa contorna, hai dous datos que nos deben levar á reflexión: case a metade dos e das menores recoñece ter aceptado algunha vez nunha rede social persoas que realmente non coñecían de nada e cando menos 1 de cada 3 chegou finalmente a ter unha cita física con estas persoas. Ambos os datos revelan un caldo de cultivo realmente perigoso e a necesidade dun esforzo específico de sensibilización

un mundo. Por eso lo importante en cada uno de esos casos no es la edad concreta a golpe de calendario, sino qué hemos hecho antes de ese momento y qué pensamos hacer a continuación, qué normas y pautas vamos a establecer. Madres y padres debemos ser muy conscientes de que detrás de todos estos nuevos dispositivos y aplicaciones hay un verdadero riesgo, no solo por los contenidos a los que nuestros hijos y nuestras hijas pueden acceder y la cantidad de líos en los que se pueden meter, sino sobre todo en lo que dejan de hacer y en el tipo de personas en que se pueden llegar a convertir. Algo tan aparentemente inocuo como un teléfono móvil ha demostrado una capacidad enorme de influir en nuestras vidas, de modificar la rutina y el estilo de vida de grandes y pequeños más allá de lo que podemos imaginar... porque al final acabamos siendo lo que hacemos cada día, las cosas en las que ocupamos cada minuto y cada hora de nuestras vidas.

¿Qué es el *grooming*?

En términos genéricos se podría decir que se trata de una nueva manera de pederastia, vinculada a Internet y a las redes sociales, que está suscitando cada vez mayor preocupación social. Se puede definir como una serie de prácticas en línea de ciertas personas adultas para ganarse la confianza de un o de una menor fingiendo empatía, cariño... con fines de satisfacción sexual; personas adultas, por ejemplo, que crean un perfil falso en una red social o en una aplicación de videojuegos en línea, haciéndose pasar por un o una menor, con la intención manifiesta de ganarse su confianza en un breve lapso de tiempo y llegar a tener finalmente un contacto sexual. Esta práctica constituye un nuevo tipo delictivo que viene recogido en la última reforma del código penitenciario, en su artículo 183.

Si bien es difícil contar con datos fiables sobre el volumen de casos existentes en las diferentes comunidades y países de nuestro entorno, hay dos datos que nos deben llevar a la reflexión: casi la mitad de los y las menores reconoce haber aceptado alguna vez en una red social a personas que realmente no conocían de nada y por lo menos 1 de cada 3 llegó a tener una cita física finalmente con estas personas. Ambos datos revelan un caldo

e na educación de cara a unha boa prevención. Comezar por entender por que os e as menores asumen riscos na Rede é o primeiro paso.

Que uso dos dispositivos electrónicos ou de Internet se considera excesivo ou problemático?

Realmente o linde entre un uso aceptable, abusivo e problemático é moitas veces difuso. Non se trata tanto de "abusar" da Rede ou do móbil nin do tempo que esteamos conectados e conectadas, senón do grao de interferencia que pode supor na vida de cada persoa. Moitas veces utilízanse de xeito indiscriminado os termos uso *abusivo,* uso *problemático,* uso *patolóxico, dependencia* ou *adición*. Convén sinalar que, a pesar de que o problema vén medrando desde hai xa dúas décadas, a día de hoxe a adición a Internet ou ao móbil non se recoñece como tal a nivel clínico, xa que non aparece recollida nos manuais diagnósticos vixentes (DSM-5). Por iso se recomenda falar de "uso problemático", porque o que si se sabe (á falta dun diagnóstico clínico) é que en moitos casos hai unha sintomática manifesta detrás, que revela que o uso do móbil ou de Internet está a producir no individuo interferencias serias na súa vida diaria e na súa contorna.

Aínda que a frecuencia e o tempo de conexión inflúen, non sempre se traducen nun problema, pero obviamente os riscos multiplícanse canto maior é o tempo de conexión ou exposición á Rede. É importante evitar un uso abusivo por parte dos e das menores. Non é unha regra exacta, pero esa é a tendencia. Segundo reflicte a propia OCDE no Informe PISA 2017, o 22% dos e das adolescentes de España pasan máis de 5 horas conectados a Internet ao día. Os últimos estudos que temos feitos en Galicia van na mesma liña, e sitúan esa porcentaxe no 29,4%. Ambos os datos son, cando menos, preocupantes. Cando avaliamos de maneira específica o posible uso problemático de Internet, empregando tests específicos, temos como resultado que a prevalencia en Galicia se sitúa moi preto do 20% (18,2%), o que quere dicir que case 1 de cada 5 mozos e mozas galegas entre 12 e 17 anos estaría a ter problemas reais co uso da Rede. Estas cifras, que son similares ás que se

de cultivo realmente peligroso y la necesidad de un esfuerzo específico de sensibilización y en la educación de cara a una buena prevención. Empezar por entender porqué los y las menores asumen riesgos en la Red es el primer paso.

¿Qué uso de los dispositivos electrónicos o de Internet se considera excesivo o problemático?

Realmente el límite entre un uso aceptable, abusivo y problemático es muchas veces difuso. No se trata tanto de "abusar" de la Red o del móvil ni del tiempo que estemos conectados y conectadas, sino del grado de interferencia que puede suponer en la vida de cada persona. Muchas veces se utilizan de manera indiscriminada los términos uso *abusivo,* uso *problemático,* uso *patológico, dependencia* o *adicción.* Conviene señalar que, a pesar de que el problema está creciendo desde hace ya dos décadas, a día de hoy la adicción a Internet o al móvil no se reconoce como tal a nivel clínico, ya que no aparece recogida en los manuales diagnósticos vigentes (DSM-5). Por eso se recomienda hablar de "uso problemático", porque lo que sí se sabe (a falta de un diagnóstico clínico) es que en muchos casos hay una sintomática manifiesta detrás, que revela que el uso del móvil o de Internet está produciendo en el individuo serias interferencias en su vida diaria y en su entorno.

Aunque la frecuencia y el tiempo de conexión influyen, no siempre se traducen en un problema, pero obviamente los riesgos se multiplican cuanto mayor es el tiempo de conexión o exposición a la Red. Es importante evitar un uso abusivo por parte de los y las menores. No es una regla exacta, pero esa es la tendencia. Según refleja la propia OCDE en el Informe PISA 2017, el 22% de los y las adolescentes de España pasan más de 5 horas conectados a Internet cada día. Los últimos estudios que hemos hecho en Galicia van en la misma línea, situando ese porcentaje en el 29,4%. Ambos datos son, por lo menos, preocupantes. Cuando evaluamos de manera específica el posible "uso problemático" de Internet, utilizando test específicos, tenemos como resultado que la prevalencia en Galicia se sitúa muy cerca del 20% (18,2%), lo que quiere decir que casi 1 de cada 5 jóvenes gallegos entre 12 y 17 años estaría teniendo problemas rea-

teñen atopado noutras comunidades e a nivel Europeo, experimentaron un lixeiro aumento nos últimos dous anos, pasando dun 16,3% a un 18,2%. A primeira lectura que debemos facer, polo tanto, é que non se trata dun problema excepcional que afecta a un grupo minoritario de adolescentes e que vai en aumento.

Como teño que actuar se o meu fillo/a é un/unha ciberacosador/a?

En primeiro lugar o que convén que teñamos claro é que o ciberacoso é algo máis frecuente do que poidamos pensar (afecta a un 10%-15% dos mozos e das mozas), e que 1 de cada 3 vítimas de ciberacoso tamén é un ou unha acosadora na Rede. Polo tanto, se o meu fillo ou a miña filla sofre ciberacoso é bastante probable que tamén estea a acosar outras persoas. As redes son un elemento potenciador e multiplicador de todo, do bo e do malo. Internet, as redes sociais, WhatsApp etc. supoñen un risco extra no acoso e dan lugar a unha tipoloxía con entidade propia, que é o chamado *cyberbullying,* que afecta cada vez a máis adolescentes.

Conviría resaltar algunhas particularidades do *cyberbullying.* É universal e accesible: o feito de que máis do 90% dos e das adolescentes teñan móbil e utilicen as redes sociais de forma habitual fai que calquera teña capacidade de acosar outras persoas a través da Rede; é anónimo e difícil de perseguir, xa que resulta sinxelo para calquera adolescente crear un perfil falso e acosar outras persoas; é 24 horas, non hai escape: a diferenza do acoso tradicional vinculado xeralmente aos centros escolares, neste caso quen acosa ten a posibilidade de "invadir" o espazo da outra persoa e de "facer dano" sen límite de horarios, polo que a persoa acosada sente que non ten escapatoria. Incluso aqueles lugares que consideraría máis seguros (como a súa casa ou o seu cuarto) pasan a ser lugares onde pode ser acosado ou acosada; é incontrolable e viral: o carácter grupal e a volatilidade da Rede fan que en moitos casos o ciberacoso teña un efecto multiplicador difícil de parar. Os elementos da ciberagresión poden manterse no tempo, xa que resulta case imposible retirar imaxes e contidos da Rede; dilución de responsabilidade, provocado por ese carácter grupal e viral, que fai que todos e todas participen en

les con el uso de la Red. Estas cifras, que son similares a las que se han encontrado en otras comunidades y a nivel europeo, experimentaron un ligero aumento en los últimos dos años, pasando de un 16,3% a un 18,2%. La primera lectura que debemos hacer, por tanto, es que no se trata de un problema excepcional que afecta a un grupo minoritario de adolescentes y que va en aumento.

¿Cómo tengo que actuar si mi hijo/a es un ciberacosador/a?

En primer lugar, lo que conviene que tengamos claro es que el ciberacoso es algo más frecuente de lo que podamos pensar (afecta a un 10%-15% de los chicos y las chicas), y que 1 de cada 3 víctimas de ciberacoso también es un o una acosadora en la Red. Por lo tanto, si mi hijo o hija sufre ciberacoso es bastante probable que también esté acosando a otra persona. Las redes son un elemento potenciador y multiplicador de todo, de lo bueno y de lo malo. Internet, las redes sociales, WhatsApp etc. suponen un riesgo extra en el acoso, dando lugar a una tipología con entidad propia, que es el llamado *cyberbullying,* que afecta cada vez a más adolescentes.

Convendría resaltar algunas particularidades del *cyberbullying.* Es universal y accesible: el hecho de que más del 90% de los y las adolescentes tengan móvil y utilicen las redes sociales de forma habitual hace que cualquier persona tenga la capacidad de acosar a otras a través de la Red; es anónimo y difícil de perseguir, ya que resulta sencillo para cualquier adolescente crear un perfil falso y acosar a otras personas; es 24 horas: no hay escape y a diferencia del acoso tradicional vinculado generalmente a los centros escolares, en este caso quien acosa tiene la posibilidad de "invadir" el espacio de otra persona y "hacer daño" sin límite de horarios, por lo que la persona acosada siente que no tiene escapatoria. Incluso aquellos lugares que consideraría más seguros (como su casa o su habitación) pasan a ser lugares donde puede ser acosado o acosada; es incontrolable y viral: el carácter grupal y la volatilidad de la Red hacen que en muchos casos el ciberacoso tenga un efecto multiplicador difícil de parar. Los elementos de la ciberagresión pueden mantenerse en el tiempo, ya que resulta casi imposible retirar imágenes

maior ou menor medida, pero que ninguén se sinta responsable; menos empático: a distancia física debilita as restricións sociais da agresión e limita a percepción do dano. O feito de que a persoa agresora non estea cara a cara coa vítima impide non só que poida defenderse, senón que a propia persoa acosadora poida percibir de forma inmediata as consecuencias dos seus actos e do dano que provoca; é planificable: dispor de medios telemáticos e da protección dunha pantalla fai que se poidan premeditar diferentes alternativas para poder acosar de maneira "máis efectiva"; máis nocivo ou daniño: o seu carácter psicolóxico fai que as consecuencias ou secuelas sexan máis severas e duradeiras, cunha maior afectación para as vítimas, derivando ás veces en depresión ou en suicidio; sentimento de invencibilidade en liña e de poder que experimenta quen agride, aumentado polo efecto desinhibidor da Rede (menores que non agredirían fisicamente, chegan a facelo a través de Internet); impulsividade: o inmediato das comunicacións provoca un aumento dos actos impulsivos, nos que apenas media pensamento, o que a miúdo deriva nunha escalada de conflito; máis difícil de detectar e solucionar para o contorno, que adoita tardar en reaccionar e buscar solucións; por último, o descoñecemento social, tanto no plano legal, xa que moita xente non sabe que se trata dun delito recollido no código penal (art. 172), como a nivel de prevención e de actuación.

Para a súa prevención fai falta un traballo transversal, no que poidan arrimar o ombro nais e pais, mestres e mestras e institucións... sen botarse a culpa mutuamente, ou reclamar para si a posesión exclusiva das solucións. Como sociedade hai moitas cousas nas que seguramente nos esteamos a equivocar, cun modelo de educación que ás veces persegue expedientes mais que persoas e onde a educación en valores e o fomento da autonomía, a responsabilidade e o pensamento crítico queda relegada a un segundo plano. Se a iso unimos a normalización da violencia nos medios de comunicación e na Rede (de onde beben cada día os nosos fillos e as nosas fillas) e a delegación de funcións de moitos pais e nais, xa temos o cóctel perfecto.

Apostar desde moi cedo por unha educación en valores, establecer normas e límites e fomentar unhas boas habilidades de

y contenidos de la Red; dilución de responsabilidad, provocado por ese carácter grupal y viral, que hace que todos y todas participen en mayor o menor medida, pero que nadie se sienta responsable; menos empático: la distancia física debilita las restricciones sociales de la agresión y limita la percepción del daño. El hecho de que la persona agresora no esté vis a vis con la víctima impide, no solo que esta pueda defenderse, sino que quien acosa pueda percibir de forma inmediata las consecuencias de sus actos y del daño que provoca; es planificable: disponer de medios telemáticos y de la protección de una pantalla hace que se puedan premeditar diferentes alternativas para poder acosar de manera "más efectiva"; más nocivo o dañino: su carácter psicológico hace que las consecuencias o secuelas sean más severas y duraderas, con una mayor afectación para las víctimas, derivando a veces en depresión o en suicidio; sentimiento de invencibilidad en línea y poder que experimenta quien agrede, aumentado por el efecto desinhibidor de la Red (menores que no agredirían físicamente, sí llegan a hacerlo a través de Internet); impulsividad: la inmediatez de las comunicaciones provoca un aumento de los actos impulsivos, en los que apenas media pensamiento, derivando a menudo en una escalada de conflicto; más difícil de detectar y solucionar para el entorno, que suele tardar en reaccionar y buscar soluciones; por último, el desconocimiento social, tanto en el plano legal, ya que mucha gente no sabe que se trata de un delito recogido en el código penitenciario (art. 172), como a nivel de prevención y de actuación.

Para su prevención hace falta un trabajo transversal, en el que puedan arrimar el hombro madres y padres, maestros y maestras e instituciones... sin echarse la culpa mutuamente, o reclamar para sí la posesión exclusiva de las soluciones. Como sociedad hay muchas cosas en las que seguramente nos estemos equivocando, con un modelo de educación que a veces persigue expedientes más que personas y donde la educación en valores y el fomento de la autonomía, la responsabilidad y el pensamiento crítico queda relegada a un segundo plano. Si a eso unimos la normalización de la violencia en los medios de comunicación y en la Red (de donde beben cada día nuestros

vida (autoestima, empatía, asertividade, habilidades de comunicación e resolución de conflitos...) son a mellor ferramenta. A prohibición e a censura non son unha boa opción. Ameazar con privar o noso fillo ou a nosa filla dos seus privilexios tecnolóxicos (castigar sen móbil unha boa tempada), tampouco o é. Segundo persoas expertas, precisamente o medo a quedar sen móbil constitúe o principal motivo de ocultación aos pais e ás nais cando un ou unha adolescente está a ser acosado ou acosada na Rede ou está a acosar outras persoas. Persoas expertas recomendan aplicar a máxima da Tripla A: Acoller, Axudar e Actuar, sancionando e corrixindo con firmeza as condutas, pero non a persoa.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Máis alá da Identidade Dixital, eu insistiría en que o que está en xogo é a educación dos nosos fillos e das nosas fillas e o seu crecemento como persoas. Internet e as redes teñen unha capacidade de modular a rutina, o estilo de vida e as pautas de socialización das novas xeracións realmente extraordinaria. Trátase non só do que fan na Rede, senón do que deixan de facer e dos modelos de referencia que aprenden nese novo contexto, neses novos patios que son as redes sociais, que supoñen unha nova maneira de vivir, de relacionarnos, de estar no mundo e de sermos. Cómpre que nos poñamos a andar, empezando por ser conscientes do que temos entre as mans. Educar a día de hoxe implica educar no uso responsable da tecnoloxía e da Rede. É preciso pararse, dedicarlle tempo, marcando normas e lindes e educando en valores máis que nunca. A misión de nais e pais pasa tamén por regular e tentar garantir un uso saudable de dispositivos móbiles, ordenadores, consolas etc. Supervisar, acompañar e establecer normas e lindes, xustamente o que non facemos. Debemos **O**bservar, **C**ontrolar, **L**imitar e **A**compañar (que é o que expertos e expertas resumimos co acrónimo **OCLA**). Tense demostrado que naquelas familias onde os pais e as nais supervisan e controlan o uso do móbil e aconsellan os seus fillos e as súas fillas, as taxas de uso problemático, de ciberacoso, de *sexting* ou de contacto con persoas descoñecidas redúcense á metade.

hijos e hijas) y la delegación de funciones de muchos padres y madres, ya tenemos el cóctel perfecto.

Apostar desde muy pronto por una educación en valores, establecer normas y límites y fomentar unas buenas habilidades de vida (autoestima, empatía, asertividad, habilidades de comunicación y resolución de conflictos...) son la mejor herramienta. La prohibición y la censura no son una buena opción. Amenazar con privar a nuestro hijo o hija de sus privilegios tecnológicos (castigarle sin móvil una buena temporada), tampoco lo es. Según personas expertas, precisamente el miedo a quedarse sin móvil constituye el principal motivo de ocultamiento a sus padres y madres cuando un o una adolescente está siendo acosado o acosada en la Red o está acosando a otras personas. Los expertos recomiendan aplicar la máxima de la Triple A: Acoger, Ayudar y Actuar, sancionando y corrigiendo con firmeza las conductas, pero no a la persona.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Más allá de la Identidad Digital, yo insistiría en que lo que está en juego es la educación de nuestros hijos e hijas y su crecimiento como personas. Internet y las redes tienen una capacidad para modular la rutina, el estilo de vida y las pautas de socialización de las nuevas generaciones realmente extraordinaria. Se trata no solo de lo que hacen en la Red, sino de lo que dejan de hacer y de los modelos de referencia que aprenden en ese nuevo contexto, en esos nuevos patios que son las redes sociales, que suponen una nueva manera de vivir, de relacionarnos, de estar en el mundo y de ser. Es necesario que nos pongamos las pilas, empezando por ser conscientes de lo que tenemos entre manos. Educar a día de hoy implica educar en el uso responsable de la tecnología y de la Red. Es necesario pararse, dedicarle tiempo, marcando normas y lindes y educando en valores más que nunca. La misión de madres y padres pasa también por regular e intentar garantizar un uso saludable de dispositivos móviles, ordenadores, consolas etc. Supervisar, acompañar y establecer normas y límites, justamente lo que no hacemos. Debemos **O**bservar, **C**ontrolar, **L**imitar y **A**compañar

Un exemplo claro témolo nos mozos e nas mozas que dormen co móbil no cuarto e adoitan conectarse a Internet de madrugada, onde todas estas prácticas de risco se multiplican por 3 ou por 4. Realmente podemos facer máis do que facemos. É un investimento que leva tempo e que dá traballo, pero paga a pena.

Entre as recomendacións que sabemos que funcionan, a primeira sería racionalizar ou retardar o acceso ao primeiro móbil, non antes dos 12 anos. O tránsito de primaria a secundaria pode ser un bo momento. Facer ademais que a chegada do móbil á súa vida diaria sexa gradual e auto regulada, establecendo unha serie de pautas (tarxeta prepagamento, non se leva ao instituto, non se dorme co móbil no cuarto, non se usa durante as comidas...); evitar a prohibición e a censura (os programas de control parental axudan pero non son a solución); falar con claridade das vantaxes e inconvenientes das tecnoloxías e tamén dos riscos; non ter medo a poñer os problemas enriba da mesa, aínda que poida xerar discusións; insistir en que deben evitar subir fotos persoais e *selfies* e non aceptar persoas descoñecidas... e, sobre todo, se queremos confianza debemos tentar respectar a súa intimidade e dialogar. Máis efectivo que pedirlle os contrasinais é que nos rexistremos xuntos e que os sigamos nas redes sociais... e paciencia, día a día. Non debemos ter medo a equivocarnos pero, sobre todo, nunca hai que tirar a toalla. Os resultados non se acadan nun día.

(que es lo que expertos y expertas resumimos con el acrónimo **OCLA**). Se ha demostrado que en aquellas familias donde padres y madres supervisan y controlan el uso del móvil y aconsejan a sus hijos e hijas, las tasas de uso problemático, de ciberacoso, de *sexting* o de contacto con personas desconocidas se reducen a la mitad. Un ejemplo claro lo tenemos en los chicos y las chicas que duermen con el móvil en la habitación y suelen conectarse a Internet de madrugada, donde todas estas prácticas de riesgo se multiplican por 3 o por 4. Realmente podemos hacer más de lo que hacemos. Es una inversión que lleva tiempo y trabajo, pero vale la pena.

Entre las recomendaciones que sabemos que funcionan, la primera sería racionalizar o retardar el acceso al primer móvil, no antes de los 12 años. El tránsito de primaria a secundaria puede ser un buen momento. Hacer además que la llegada del móvil a su vida diaria sea gradual y autoregulada, estableciendo una serie de pautas (tarjeta prepago, no se lleva al instituto, no se duerme con el móvil en la habitación, no se usa durante las comidas...); evitar la prohibición y la censura (los programas de control parental ayudan pero no son la solución); hablar con claridad de las ventajas e inconvenientes de las tecnologías y también de los riesgos; no tener miedo a poner los problemas encima de la mesa, aunque pueda generar discusiones; insistir en que deben evitar subir fotos personales y selfies y no aceptar a personas desconocidas... y, sobre todo, si queremos confianza debemos intentar respetar su intimidad y dialogar. Más efectivo que pedirle las contraseñas es que nos registremos juntos y que los sigamos en las redes sociales... y paciencia, día a día. No debemos tener miedo a equivocarnos, pero, sobre todo, nunca hay que tirar la toalla. Los resultados no se alcanzan en un día.

CARMEN AMPARO RODRÍGUEZ LOMBARDÍA

Licenciada en Medicina e Cirurxía pola Universidade de Santiago, especialista en Pediatría vía MIR (Hospital Materno-Infantil Teresa Herrera). Pediatra de Atención Primaria no CS Casa do Mar, relatora e moderadora de diversos cursos e titora de residentes de Medicina de Familia e Pediatría en Atención Primaria. Coordinadora dos cursos de Formación Continuada en Pediatría, desde o ano 2008.

Proxecto de investigación de Prevalencia de Patoloxía Psiquiátrica en consultas de pediatría de atención primaria en Galicia.

Presidenta da AGAPAP (Asociación Galega de Pediatría de Atención Primaria) e vogal da AEPAP (Asociación Española de Pediatría de Atención Primaria).

Licenciada en Medicina y Cirugía por la Universidad de Santiago, especialista en Pediatría vía MIR (Hospital Materno-Infantil Teresa Herrera). Pediatra de Atención Primaria en el CS Casa del Mar, ponente y moderadora de diversos cursos y tutora de residentes de Medicina de Familia y Pediatría en Atención Primaria. Coordinadora de los cursos de Formación Continuada en Pediatría desde el año 2008.

Proyecto de investigación de Prevalencia de Patología Psiquiátrica en consultas de pediatría de atención primaria en Galicia.

Presidenta de la AGAPAP (Asociación Gallega de Pediatría de Atención Primaria) y vocal de la AEPAP (Asociación Española de Pediatría de Atención Primaria).

Como integramos o consumo de contidos dixitais nunha infancia saudable?

Inculcándolle aos nosos fillos e fillas, alumnado ou pacientes os principios e valores polos que nos debemos rexer tanto no mundo real como no dixital. Debemos educar no respecto, na coherencia, na responsabilidade e na tolerancia.

Os contidos aos que accede un ou unha menor deben de ser adecuados á súa idade. Debemos coñecer e usar ferramentas de control parental, desde a supervisión total a unha estreita supervisión, axustando o nivel de mediación ao nivel de maduración.

É necesario establecer regras e límites, equilibrio co resto das actividades do ou da menor. Non permitamos que abandone outras actividades ou amigos e amigas reais.

Favorecer o pensamento crítico. Non sempre é certo o que sae en Internet. As persoas descoñecidas non son as nosas amigas.

Ser capaces de transmitirlle aos nosos menores e ás nosas menores que o que se colga nas redes é das redes. E que esa pegada dixital pode ter consecuencias para as súas relacións e para o seu futuro. Respecto pola súa propia privacidade e pola dos demais.

¿Cómo integramos el consumo de contenidos digitales en una infancia sana?

Inculcando a nuestros hijos e hijas, alumnado o pacientes los principios y valores por los que nos debemos regir tanto en el mundo real como en el digital. Debemos educar en el respeto, en la coherencia, en la responsabilidad y en la tolerancia.

Los contenidos a los que accede un o una menor deben ser adecuados a su edad. Debemos conocer y usar herramientas de control parental, desde la supervisión total a una estrecha supervisión, ajustando el nivel de mediación al nivel de maduración.

Es necesario establecer reglas y límites, equilibrio con el resto de las actividades del o de la menor. No permitamos que abandone otras actividades o amigos y amigas reales.

Favorecer el pensamiento crítico. No siempre es cierto lo que sale en Internet. Las personas desconocidas no son nuestras amigas.

Ser capaces de transmitir a nuestros menores y nuestras menores que lo que se cuelga en las redes es de las redes. Y que esa huella digital puede tener consecuencias para sus relaciones y para su futuro. Respeto por su propia privacidad y la de los demás.

Cando debe preocuparse unha familia ou o profesorado por un posible uso abusivo de Internet?

Cando detectamos problemas físicos (dor de costas, fatiga ocular, cefalea, trastornos do sono...), académicos (falta de concentración, fracaso escolar..), psíquico-sociais (agresividade, apatía, illamento, cambios no comportamento...).

Que axuda poden ofrecer os servizos de saúde cando as familias ou os centros detectan que a contorna dixital pode causar problemas ao alumnado?

Dentro do Programa de Saúde Infantil debemos realizar prevención primaria falando con pais, nais e menores dos riscos e dos beneficios das redes sociais.

Debemos ser persoas activas na procura de signos que nos poidan alertar na consulta de posibles vítimas ou autores de delitos que se cometen nas redes: cambios físicos, emocionais ou do comportamento dos nosos e das nosas doentes.

Diante da sospeita dun caso de ciberacoso, *grooming*... debemos actuar inmediatamente.

Documentalo.

Valorar a gravidade.

Valorar risco paciente: falar co menor ou coa menor, evitar culpabilización, transmitir confianza, pactar con el ou con ela os pasos que se van seguir.

Buscar os apoios necesarios para axudar ao ou á menor.

Prestarlle axuda psicolóxica e tratamento de o precisar.

Denunciar.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Non deixes o teu fillo ou a túa filla/alumnado en soidade diante das TIC. Acompaña no bo uso, sen abuso e con responsabilidade das novas tecnoloxías.

¿Cuándo debe preocuparse una familia o el profesorado por un posible uso abusivo de Internet?

Cuando detectamos problemas físicos (dolor de espalda, fatiga ocular, cefalea, trastornos del sueño...), académicos (falta de concentración, fracaso escolar...), psíquico-sociales (agresividad, apatía, aislamiento, cambios en el comportamiento...).

¿Qué ayuda pueden ofrecer los servicios de salud cuando las familias o los centros detectan que el entorno digital puede causar problemas al alumnado?

Dentro del Programa de Salud Infantil debemos realizar prevención primaria hablando con los padres, las madres y los y las menores de riesgos y beneficios de las redes sociales.

Debemos ser personas activas en la búsqueda de signos que nos puedan alertar en la consulta de posibles víctimas o autores de delitos que se cometen en redes: cambios físicos, emocionales o del comportamiento de nuestros enfermos y enfermas.

Ante la sospecha de un caso de ciberacoso, *grooming*... debemos actuar inmediatamente.

Documentarlo.

Valorar la gravedad.

Valorar riesgo paciente: hablar con el o la menor, evitar culpabilización, transmitir confianza, pactar con él o ella los pasos a seguir.

Buscar los apoyos necesarios para ayudar al o a la menor.

Prestarle ayuda psicológica y tratamiento si lo necesita.

Denunciar.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

No dejes a tu hijo o hija/alumnado en soledad ante las TIC. Acompaña en el buen uso, sin abuso y con responsabilidad de las nuevas tecnologías.

VÍCTOR SALGADO SEGUÍN

Socio-Director de Pintos & Salgado Avogados.

Especializado en Dereito TIC desde 1997.

Socio-Director de Pintos & Salado Abogados.

Especializado en Derecho TIC desde 1997.

A imaxe persoal (propia imaxe) está protexida polo dereito á intimidade?

Non só está protexida senón que, de feito, goza dun dereito fundamental propio recoñecido no artigo 18 da nosa Constitución: trátase do dereito á propia imaxe.

Este é un dereito bastante descoñecido, salvo que falemos no ámbito das dúas grandes efes: Famosos e Futbolistas. Isto é porque, devanditos colectivos viven, directa ou indirectamente, da súa propia imaxe a nivel profesional pero, curiosamente, son os colectivos que menos están protexidos por este dereito fundamental. A razón é moi simple: o que protexe principalmente este dereito fundamental é o anonimato, é dicir, o dereito de toda persoa a camiñar tranquilamente pola rúa sen que ninguén, salvo os seus coñecidos, saiban quen é.

Por tanto, o dereito á o propia imaxe prohibe, a efectos prácticos, que ninguén poida sacar unha fotografía a unha persoa, e moito menos publicala, sen a súa previa autorización. E isto salvo excepcións moi concretas como o caso das persoas famosas, en determinados ámbitos, ou as imaxes tomadas por un medio de comunicación, sempre que a imaxe dunha persoa sexa meramente accesoria.

En efecto, este é un dos dereitos máis vulnerado nos últimos anos con ocasión da proliferación das redes sociais e da práctica estendida de tomar e subir fotos sen autorización, incluíndo as dos menores.

A lei de protección de datos española, como se vincula coas políticas de privacidade?

Para empezar, o termo "política de privacidade" é máis aplicable á contorna normativa de EEUU (da cal procede) que non á contorna europea. En Estados Unidos non hai unha Lei de Protección de Datos a nivel Federal, como a Directiva, o Re-

¿La imagen personal (propia imagen) está protegida por el derecho a la intimidad?

No solo está protegida, sino que, de hecho, goza de un derecho fundamental propio reconocido en el artículo 18 de nuestra Constitución: se trata del derecho a la propia imagen.

Este es un derecho bastante desconocido, salvo que hablemos en el ámbito de las dos grandes efes: personas Famosas y Futbolistas. Esto es porque dichos colectivos viven, directa o indirectamente, de su propia imagen a nivel profesional, pero, curiosamente, son los colectivos que menos están protegidos por este derecho fundamental. La razón es muy simple: lo que protege principalmente este derecho fundamental es el "anonimato", es decir, el derecho de toda persona a caminar tranquilamente por la calle sin que nadie, salvo las personas que la conocen, sepan quién es.

Por tanto, el derecho a la propia imagen prohíbe, a efectos prácticos, que nadie pueda sacar una fotografía a una persona, y mucho menos publicarla, sin su previa autorización. Y esto salvo excepciones muy concretas como el caso de las personas famosas, en determinados ámbitos, o las imágenes tomadas por un medio de comunicación, siempre que la imagen de una persona sea meramente accesoria.

En efecto, este es uno de los derechos más vulnerados en los últimos años con ocasión de la proliferación de las redes sociales y de la práctica extendida de tomar y subir fotos sin autorización, incluyendo las de menores.

La ley de protección de datos española, ¿cómo se vincula con las políticas de privacidad?

Para empezar, el término de "política de privacidad" es más aplicable al entorno normativo de EEUU (del cual procede) que no al entorno europeo. En Estados

gulamento Europeo ou a LOPD española. Por tanto, cando non temos unha Lei de Privacidade, que temos? Pois temos unha *política de privacidade.* É dicir, unha norma autoimposta e non limitada por unha lei formal onde eu simplemente conto como vou tratar os datos na miña organización. Nesta contorna, a única limitación que teño é a de "contar a verdade e toda a verdade" aos interesados e, no seu caso, solicitar o seu consentimento ou aceptación desa política.

Aquí é onde temos a maior mentira de Internet que non é outra que "lin atentamente e acepto as condicións de uso". E é que todos, ou case todos, aceptamos as ditas condicións, política de privacidade incluída, sen nin sequera botarlle unha lectura superficial, e así nos atopamos logo as sorpresas.

Con todo, no que a Europa e a España se refire, a dita política de privacidade non ten o mesmo sentido xa que non pode conter o que á organización *lle dea a gana* senón só aquilo que cumpra estritamente o contido e requisitos dispostos na Lei. Por tanto, aquí é menos grave se non nos lemos as ditas condicións xa que sempre teñen que respectar un mínimo de protección e obrigacións impostas legalmente. Por iso falamos de Protección de Datos, a diferenza doutras contornas xurídicas menos restritivas.

Calquera persoa pode subir a internet unha foto nosa sempre que non nos etiquete? E se nos etiqueta? E cando se sobe a un xornal?

Tal e como comentamos na primeira resposta, ninguén pode captar nin, por suposto, subir a fotografía dunha persoa a unha rede social sen o previo consentimento concreto da mesma. Neste sentido, dá igual que a etiquete ou non porque o dereito á propia imaxe está vulnerado igualmente. En todo caso, falariamos dunha responsabilidade engadida por vulnerar tamén o dereito á privacidade da devandita persoa ao etiquetala tamén.

No caso dun xornal, como indicamos tamén, é distinto posto que está a exercer un dereito tamén fundamental como é a liberdade de información e a liberdade de expresión. Por iso, a Lei Orgánica 1/1982, no seu artigo 8.2.c), permite que un xornal poida publicar fotografías de

Unidos, no hay una ley de protección de datos a nivel federal, como la Directiva, el Reglamento Europeo o la LOPD española. Por tanto, cuando no tenemos una "ley de privacidad", ¿qué tenemos? Pues tenemos una *"política de privacidad".* Es decir, una norma autoimpuesta y no limitada por una ley formal donde yo simplemente cuento cómo voy a tratar los datos en mi organización. En este entorno, la única limitación que tengo es la de "contar la verdad y toda la verdad" a las personas interesadas y, en su caso, recabar su consentimiento o aceptación de esa política.

Aquí es donde tenemos la mayor mentira de internet que no es otra que el "he leído atentamente y acepto las condiciones de uso". Y es que todas las personas usuarias, o casi todas, aceptamos dichas condiciones, "política de privacidad" incluida, sin ni siquiera echarle una lectura superficial y así nos encontramos luego las sorpresas.

Sin embargo, en lo que a Europa y a España se refiere, dicha política de privacidad no tiene el mismo sentido ya que no puede contener lo que a la organización *"le dé la gana"* sino sólo aquello que cumpla estrictamente el contenido y requisitos dispuestos en la Ley. Por tanto, aquí es menos grave si no nos leemos dichas condiciones ya que siempre tienen que respetar un mínimo de protección y obligaciones impuestas legalmente. Por ello hablamos de "Protección de Datos", a diferencia de otros entornos jurídicos menos restrictivos.

¿Cualquier persona puede subir a Internet una foto nuestra siempre que no nos etiquete? ¿Y si nos etiqueta? ¿Y cuando se sube a un periódico?

Tal y como comentamos en la primera respuesta, nadie puede captar ni, por supuesto, subir la fotografía de una persona a una red social sin el previo consentimiento concreto de la misma. En este sentido, da igual que la etiquete o no porque el derecho a la propia imagen está vulnerado igualmente. En todo caso, hablaríamos de una responsabilidad añadida por vulnerar también el derecho a la privacidad de dicha persona al etiquetarla.

En el caso de un periódico, como indicamos, es distinto puesto que está ejer-

persoas pero sempre que se cumpran dúas condicións:

1. Que sexa para informar dun suceso ou acaecemento público (obxecto noticiable) e
2. Que a imaxe dunha persoa concreta sexa meramente accesoria e non o centro da noticia (salvo no caso de personaxes públicos definidos na xurisprudencia constitucional posterior).

Para poder exercer os nosos dereitos o mellor é utilizar sempre o noso nome real

Isto non é necesario. En internet tamén temos dereito a publicar anonimamente ou baixo pseudónimo. Ninguén está obrigado a identificarse salvo para accións e trámites moi concretos e conforme a Lei.

Iso si, dicir que temos dereito a ser anónimos non implica que gocemos dun anonimato total ou de total impunidade respecto do que publiquemos ou fagamos a través da rede. Como na vida real, todo o que facemos na Rede deixa un rastro e, en caso de ser necesario e en aplicación dos instrumentos legais, podemos chegar a ser identificados e, mesmo, perseguidos para a investigación de determinadas infraccións ou delitos cometidos en Internet como, por exemplo, a publicación de contidos ilícitos ou nocivos en prexuízo doutras persoas.

Se usamos un pseudónimo e facemos declaracións falsas ou vertemos insultos contra alguén que tamén usa pseudónimo, non pode haber delito.

Ao contrario. En base ao comentado na resposta anterior, calquera falsidade ou insulto vertido contra outra persoa desde un pseudónimo ou desde o anonimato é igualmente un delito e non se beneficia de ningunha impunidade total ou parcial por iso. Do mesmo xeito, aínda que a vítima use igualmente un pseudónimo ou sexa anónima, iso non quere dicir que non exista responsabilidade. O motivo é que, detrás dese pseudónimo, hai unha persoa con dereitos que poden ser vulnerados e, por tanto, é igualmente perseguible. O dereito á honra dunha persoa ten tanto unha vertente pública, a reputación da mesma na sociedade, como unha vertente privada, a súa dig-

ciendo un derecho también fundamental como es la libertad de información y la libertad de expresión. Por ello, la Ley Orgánica 1/1982, en su artículo 8.2.c), permite que un periódico pueda publicar fotografías de personas, pero siempre que se cumplan dos condiciones:

1. Que sea para informar de un suceso o acontecimiento público (objeto noticiable) y
2. Que la imagen de una persona concreta sea meramente accesoria y no el centro de la noticia (salvo en el caso de personajes públicos definidos en la jurisprudencia constitucional posterior).

Para poder ejercer nuestros derechos lo mejor es utilizar siempre nuestro nombre real.

Esto no es necesario. En internet también tenemos derecho a publicar anónimamente o bajo seudónimo. Nadie tiene la obligación de identificarse salvo para acciones y trámites muy concretos y con arreglo a la Ley.

Eso sí, decir que tenemos derecho al anonimato no implica que disfrutemos de un anonimato total o de total impunidad respecto a lo que publiquemos o hagamos a través de la red. Como en la vida real, todo lo que hacemos en la Red deja un rastro y, en caso de ser necesario y en aplicación de los instrumentos legales, puede ser que nos identifiquen e, incluso, persigan para la investigación de determinadas infracciones o delitos cometidos en internet como, por ejemplo, la publicación de contenidos ilícitos o nocivos en perjuicio de otras personas.

Si usamos un seudónimo y hacemos declaraciones falsas o proferimos insultos contra alguien que también usa seudónimo, no puede haber delito.

Al contrario. En base a lo comentado en la respuesta anterior, cualquier falsedad o insulto vertido contra otra persona desde un seudónimo o desde el anonimato es igualmente un delito y no se beneficia de ninguna impunidad total o parcial por ello. Del mismo modo, aunque la víctima use igualmente un seudónimo o sea anónima, eso no quiere decir que no exista responsabilidad. El motivo es que, detrás de ese seudónimo, hay una persona con

nidade e amor propio e isto último pode ser vulnerado e afectado igualmente en todos os casos.

Como ben resumiu Virginia Shea, autora norteamericana que publicou un libro sobre as primeiras regras de comportamento en Internet, chamado *NETiquette* nos 90, a primeira delas é: "Nunca esqueza que a persoa que le a mensaxe é en efecto humana con sentimentos que poden ser magoados".

Por que Facebook/Twitter/ Instagram/Google... son gratuítos?

Esta é unha grande pregunta que todos deberiamos facernos hoxe en día. O motivo é que, en realidade, non son gratuítos, senón que pagamos con outra moeda: os nosos datos. Os devanditos datos, grazas á "maior mentira de Internet" que comentabamos antes, extráense de maneira masiva e altamente intrusiva sobre nós e véndense ao mellor ofertante, literalmente.

Este é un modelo de negocio que está a imperar en Internet, grazas especialmente á permisiva lexislación norteamericana, que conleva que os usuarios destas plataformas nos convertamos, en realidade, nos verdadeiros produtos que estas compañías venden aos seus verdadeiros clientes: os anunciantes. O Gran Irmán de Orwell está máis preto do que cremos. Para protexernos, afortunadamente está a lexislación europea, que recentemente estreou un novo Regulamento UE que entrará plenamente en aplicación o 25 de maio de 2018 pero que, como interesados, debemos coñecer e esixir, e utilizar activamente as ferramentas que nos confire para protexernos.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

O meu consello sería o de deixar de ter medo á tecnoloxía e de idolatrar á falsa figura do nativo dixital, para realmente tomar coñecemento dela e ensinar aos menores a usala dun modo responsable e con plena conciencia dos nosos dereitos e total respecto aos alleos. Temos a mellor ferramenta da Historia da Humanidade, só temos que aprender e ensinar a utilizala ben.

derechos que pueden ser vulnerados y, por tanto, es igualmente perseguible. El derecho al honor de una persona tiene tanto una vertiente pública, la reputación de la misma en la sociedad, como una vertiente privada, su dignidad y amor propio y esto último puede ser vulnerado y afectado igualmente en todos los casos.

Como bien resumió Virginia Shea, autora norteamericana que publicó un libro sobre las primeras reglas de comportamiento en internet, llamado *"NETiquette"* en los 90, la primera de ellas es: "Nunca olvide que la persona que lee el mensaje es en efecto humana con sentimientos que pueden ser dañados".

¿Por qué Facebook/Twitter/ Instagram/Google... son gratuitos?

Esta es una gran pregunta que deberíamos hacernos hoy en día. El motivo es que, en realidad, no son gratuitos, sino que pagamos con otra moneda: nuestros datos. Dichos datos, gracias a "la mayor mentira de internet" que comentábamos antes, se extraen de manera masiva y altamente intrusiva sobre nosotros y se venden al mejor postor, literalmente.

Este es un modelo de negocio que está imperando en internet, gracias especialmente a la permisiva legislación norteamericana, que implica que las personas usuarias de estas plataformas nos convirtamos, en realidad, en los verdaderos productos que estas compañías venden a su verdadera clientela: los y las anunciantes. El Gran Hermano de Orwell está más cerca de lo que creemos. Para protegernos, afortunadamente, está la legislación europea, que recientemente ha estrenado un nuevo Reglamento UE que entrará plenamente en aplicación el 25 de mayo de 2018 pero que, como personas interesadas, debemos conocer y exigir y utilizar activamente las herramientas que nos confiere para protegernos.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Mi consejo sería el de dejar de tener miedo a la tecnología y de idolatrar a la falsa figura del nativo o nativa digital, para realmente tomar conocimiento de ella y enseñar a los y las menores a usarla de un modo responsable y con plena conciencia de nuestros derechos y total respeto a los

ajenos. Tenemos la mejor herramienta de la Historia de la Humanidad, sólo tenemos que aprender y enseñar a utilizarla bien.

FERNANDO SUÁREZ LORENZO

Licenciado en Informática pola Universidade da Coruña, é un dos impulsores do Colexio Profesional de Enxeñaría en Informática de Galicia (CPEIG), órgano que preside desde a súa constitución, en decembro de 2007.

Desde maio de 2016 desenvolve a súa actividade profesional na Axencia de Modernización Tecnolóxica de Galicia (AMTEGA) da Xunta de Galicia, como xefe do Departamento de Sistemas. Previamente, desde 2006, traballou no Concello Santiago de Compostela, primeiro como xefe de Sistemas e Comunicacións e posteriormente como xefe de Innovación, liderando o proxecto Smart iAgo, estratexia de Smart City nunha Cidade Patrimonio. Actualmente é tamén vicepresidente 1º do Consello Xeral de Colexios de Enxeñaría en Informática, cargo no que permanece desde 2009.

Licenciado en Informática por la Universidad de A Coruña, es uno de los impulsores del Colegio profesional de Ingeniería en Informática de Galicia (CPEIG), órgano que preside desde su constitución, en diciembre de 2007.

Desde mayo de 2016 desarrolla su actividad profesional en la Agencia de Modernización Tecnológica de Galicia (AMTEGA) de la Xunta de Galicia, como jefe del Departamento de Sistemas. Previamente, desde 2006, trabajó en el Ayuntamiento Santiago de Compostela, primero como jefe de Sistemas y Comunicaciones y posteriormente como jefe de Innovación, liderando el proyecto Smart iAgo, estrategia de Smart City en una Ciudad Patrimonio. Actualmente es también vicepresidente 1º del Consejo General de Colegios de Ingeniería en Informática, cargo en el que permanece desde 2009.

Un/Unha menor de 18 anos pode ter conta en redes sociais?

No noso país, a idade mínima para poder abrir un perfil nunha rede social está establecida nos 14 anos, tal e como se recolle no Regulamento que desenvolve a LOPD (Lei Orgánica de Protección de Datos de Carácter Persoal). Por debaixo desa idade é necesario o consentimento dos pais, das nais ou titores. Non obstante, o novo Regulamento Xeral de Protección de Datos (RGPD), que obrigará á actualización da LOPD, vixente desde 1999, establece a idade mínima nos 16 anos, pero permitindo que os Estados Membros a fixen con anterioridade, aínda que sempre por riba dos 13 anos. Este regulamento comezará a súa aplicación o 25 de maio de 2018.

Esta situación antóllase complicada por dous factores: por unha banda, a comprobación de idade é realmente complexa en Internet a día de hoxe, xa que son claramente insuficientes os mecanismos actuais de consulta de idade nos que unha resposta que indique menos de 14 anos impide o acceso (se a condición necesaria para crear un perfil nunha rede social é ter esta idade, ningún menor recoñecerá ter menos anos); por outra, é unha quimera esixir control paterno ou materno

Un/a menor de 18 años, ¿puede tener cuenta en redes sociales?

En nuestro país, la edad mínima para poder abrir un perfil en una red social está establecida en los 14 años, tal y como se recoge en el Reglamento que desarrolla la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal). Por debajo de esa edad es necesario el consentimiento de los padres, de las madres o tutores. No obstante, el nuevo Reglamento General de Protección de Datos (RGPD), que obligará a la actualización de la LOPD, vigente desde 1999, establece la edad mínima en los 16 años, pero permitiendo que los Estados Miembros la fijen con anterioridad, aunque siempre por encima de los 13 años. Este reglamento comenzará su aplicación el 25 de mayo de 2018.

Esta situación se antoja complicada por dos factores: por una parte, la comprobación de edad es realmente compleja en Internet a día de hoy, siendo claramente insuficientes los actuales mecanismos de consulta de edad en los que una respuesta que indique menos de 14 años impide el acceso (si la condición necesaria para crear un perfil en una red social es tener esta edad, ningún menor reconocerá tener menos años); por otra, es una quime-

para cada decisión na Rede dun ou dunha adolescente do século XXI.

Todo o contido publicado en Internet é libre.

En primeiro lugar, habería que definir que é o contido libre en Internet. Poderíase definir como aquel contido ou información que non posúe restricións legais significativas en relación co dereito de uso, redistribución e creación de versións modificadas por parte de terceiras persoas.

Polo tanto, hai unha diferenza importante en que o acceso a certos contidos sexa libre, con que o uso destes contidos teña a mesma cualificación. Por exemplo, se un autor ou unha autora publica unha obra en Internet (musical, literaria...) non necesariamente este contido é libre, xa que está suxeito ás restricións de dereitos de autoría, de modo que se quixese que a publicación fose libre, tería que declarar de forma explícita este feito. Isto é, por exemplo, o que ocorre coas licenzas *Creative Commons,* que permiten aos autores e ás autoras autorizar o uso da súa obra, pero manténdoa protexida.

Cal é a diferenza entre libre e gratuíto?

Aínda que pode parecer que son o mesmo, e de feito moita xente así o entende, son conceptos totalmente diferentes. Quizais a confusión proveña do uso da palabra inglesa "*free*", que se traduciu por ambos os dous termos, moitas veces de forma errónea.

Que un contido sexa gratuíto o que indica é que non hai que pagar polo seu uso, o que non implica necesariamente que sexa libre nos termos de liberdade explicados anteriormente, xa que o feito da súa gratuidade non outorga máis dereitos sobre os contidos en cuestión. Por outra banda, que algo sexa libre e nos permita a súa redifusión ou modificación, non implica que non teñamos que pagar polo seu uso.

Poñamos un caso práctico: podemos acceder a unha determinada canción en Internet, como ocorre no caso de YouTube, sen pagar por ela, pero iso non nos dá dereito para usala como queiramos, por exemplo para un anuncio publicitario, sen autorización do autor ou da autora. Este sería un exemplo de contido gratuíto pero non libre. Por outra banda, no caso libre

ra exigir control paterno o materno para cada decisión en la Red de un o una adolescente del siglo XXI.

Todo el contenido publicado en Internet es libre.

En primer lugar, habría que definir qué es el contenido libre en Internet. Podría definirse como aquel contenido o información que no posee restricciones legales significativas en relación con el derecho de uso, redistribución y creación de versiones modificadas por parte de terceras personas.

Por tanto, hay una diferencia importante en que el acceso a ciertos contenidos sea libre, con que el uso de los mismos tenga la misma calificación. Por ejemplo, si un autor o una autora publica una obra en Internet (musical, literaria...) no necesariamente este contenido es libre, ya que está sujeto a las restricciones de derechos de autoría, de modo que, si quisiera que la publicación fuera libre, tendría que declarar de forma explícita este hecho. Esto es, por ejemplo, lo que ocurre con las licencias *Creative Commons,* que permiten a los autores y a las autoras autorizar el uso de su obra, pero manteniéndola protegida.

¿Cuál es la diferencia entre libre y gratuito?

Aunque puede parecer que son lo mismo, y de hecho mucha gente así lo entiende, son conceptos totalmente diferentes. Tal vez la confusión provenga del uso de la palabra inglesa *"free"*, que fue traducida por ambos términos, muchas veces de forma errónea.

Que un contenido sea gratuito lo que indica es que no hay que pagar por su uso, lo que no implica necesariamente que sea libre en los términos de libertad explicados anteriormente, ya que el hecho de su gratuidad no otorga más derechos sobre los contenidos en cuestión. Por otra parte, que algo sea libre y nos permita su redifusión o modificación, no implica que no tengamos que pagar por su uso.

Pongamos un caso práctico: podemos acceder a una determinada canción en Internet, como ocurre en el caso de YouTube, sin pagar por ella, pero eso no nos da derecho para usarla como queramos, por ejemplo, para un anuncio publicitario, sin autorización del autor o de la autora. Este

vs. gratuíto, alguén pode publicar unha aplicación con formato libre, que permite a súa redifusión ou modificación para a súa mellora, e porén, cobrar por ela.

Que é o software "pirata"?

Son aqueles programas ou aplicacións que foron modificados ou distribuídos sen autorización. Exemplos de "piratería" de software poden ser a distribución de múltiples copias dun único software ou a instalación dunha única copia en varios equipos empregando a mesma licenza.

O problema do "software pirata" é que moitas veces a xente non é consciente do esforzo que supón desenvolver unha aplicación informática e que o seu autor ou autora ten dereito a unha contraprestación económica por parte de quen a utiliza. Pero tamén o "software pirata" é un dos grandes perigos na actualidade, xa que non hai garantías de quen o puido modificar e, por tanto, pode supor unha porta de entrada a virus, troianos e outros tipos de códigos maliciosos que poden poñer o noso equipo en risco. Unha das principais recomendacións que se acostuma facer no ámbito da ciberseguridade é evitar este tipo de aplicativos.

Se puideses dar un só consello ás familias e ao profesorado a respecto da identidade dixital, cal sería?

Que usen o sentido común. A contorna dixital non é en esencia tan distinta á física, polo tanto non son necesarios grandes coñecementos tecnolóxicos para poder transmitir pautas de comportamento aos rapaces e ás rapazas. Do mesmo xeito que aos nenos e ás nenas da miña xeración nos instruían a non falar con persoas estrañas, ese mesmo consello pode darse aos e ás adolescentes actuais no uso que fan das redes sociais. O mesmo ocorre co coñecemento dos amigos e das amigas dos nosos fillos e das nosas fillas, ou con saber os lugares aos que acoden. Cambia o medio (de físico a virtual), pero a esencia do comportamento é a mesma.

Ese sentido común amósase tamén no uso que as persoas adultas facemos de Internet e que serve de exemplo para os rapaces e as rapazas: se un pai ou unha nai publica contidos dos seus fillos e das súas fillas desde a infancia de forma indiscriminada, como pasa con certa frecuen-

sería un ejemplo de contenido gratuito, pero no libre. Por otra parte, en el caso libre vs. gratuito, alguien puede publicar una aplicación con formato libre, que permite su redifusión o modificación para su mejora, y, sin embargo, cobrar por ella.

¿Qué es el software "pirata"?

Son aquellos programas o aplicaciones que fueron modificados o distribuidos sin autorización. Ejemplos de "piratería" de software pueden ser la distribución de múltiples copias de un único software o la instalación de una única copia en varios equipos empleando la misma licencia.

El problema del "software pirata" es que muchas veces la gente no es consciente del esfuerzo que supone desarrollar una aplicación informática y que el autor o la autora de la misma tiene derecho a una contraprestación económica por parte de quienes la utilizan. Pero también el "software pirata" es uno de los grandes peligros en la actualidad, ya que no hay garantías de quien lo pudo modificar y, por tanto, puede suponer una puerta de entrada a virus, troyanos y otros tipos de códigos maliciosos que pueden poner nuestro equipo en riesgo. Una de las principales recomendaciones que se suele hacer en el ámbito de la ciberseguridad es evitar este tipo de aplicativos.

Si pudieses dar un único consejo a las familias y profesorado a respecto de la identidad digital, ¿cuál sería?

Que usen el sentido común. El entorno digital no es en esencia tan distinto al físico, por tanto, no son necesarios grandes conocimientos tecnológicos para poder transmitir pautas de comportamiento a los y las jóvenes. Al igual que a los niños y las niñas de mi generación nos instruían en no hablar con personas extrañas, ese mismo consejo puede darse a los y las adolescentes actuales en el uso que hacen de las redes sociales. Lo mismo ocurre con el conocimiento de los amigos y las amigas de nuestros hijos e hijas, o con saber los lugares a los que acuden. Cambia el medio (de físico a virtual), pero la esencia del comportamiento es la misma.

Ese sentido común se muestra también en el uso que las personas adultas hacemos de Internet y que sirve de ejemplo a los y las jóvenes: si un padre o una madre publica contenidos de sus hijos o hijas

cia, dificilmente vai poder establecerlles regras con certos límites no futuro.

Polo tanto, é fundamental que familias e educadores ou educadoras perdan o medo á tecnoloxía e saiban establecer unha relación de confianza e proximidade para poder ser a primeira referencia ante calquera risco ou comportamento perigoso, xa que a súa experiencia vital como adultos e adultas é moito máis importante do que pensan e dos propios coñecementos técnicos. Temos que ser conscientes que nin os profesionais e as profesionais do sector da informática somos quen de competir coa capacidade de actualización dos nosos e das nosas menores, e que Internet e as redes sociais están aquí para quedar e cada vez terán maior uso. Por todo isto o que temos as persoas adultas é outro tipo de habilidades que son fundamentais para mitigar os riscos e evitar situacións perigosas que debemos saber aproveitar.

desde su infancia de forma indiscriminada, como pasa con cierta frecuencia, difícilmente va a poder establecerles reglas con ciertos límites en el futuro.

Por tanto, es fundamental que familias y educadores o educadoras pierdan el miedo a la tecnología y sepan establecer una relación de confianza y cercanía para poder ser la primera referencia ante cualquier riesgo o comportamiento peligroso, ya que su experiencia vital como adultos y adultas es mucho más importante de lo que piensan y de los propios conocimientos técnicos. Tenemos que ser conscientes de que ni las personas profesionales del sector de la informática somos quien de competir con la capacidad de actualización de nuestros y nuestras menores, y que Internet y las redes sociales están aquí para quedarse y cada vez tendrán mayor uso. Por todo esto, lo que tenemos las personas adultas es otro tipo de habilidades que son fundamentales para mitigar los riesgos y evitar situaciones peligrosas que debemos saber aprovechar.

ÍNDICE DE PREGUNTAS

900 116 117

O Instituto Nacional de Ciberseguridade (INCIBE), ten activada unha liña de asistencia telefónica 900 116 117 para resolver as dúbidas e conflitos que habitualmente xorden no uso de Internet e as tecnoloxías por parte de nenos e nenas, adolescentes e os seus pais e nais.

Esta liña de asesoramento telefónico está atendida por expertos en psicoloxía, seguridade das tecnoloxías e cuestións legais. As chamadas atenderanse en horario de 10:00 a 20:00 horas de luns a venres e de 10:00 a 14:00 horas os sábados. Ademais, durante as 24 horas do día, os usuarios poden remitir dúbidas e consultas ao enderezo de correo electrónico ayuda@is4k.es.

Este servizo, de carácter confidencial e gratuíto, proporciona á menores asistencia sobre calquera consulta relacionada co uso seguro e responsable de Internet e os seus riscos como poden ser os conflitos sobre privacidade e reputación, o ciberbullying, o uso excesivo, contidos e contactos inapropiados, comunidades perigosas, así como cuestións sobre protección de dispositivos, virus ou fraudes, entre outros.

Xunto a nenos e adolescentes, tamén poderán facer chamadas pais, educadores e profesionais do ámbito do menor e atopar axuda para facer fronte a calquera circunstancia que poida xurdir en relación ao uso de Internet.

El Instituto Nacional de Ciberseguridad (INCIBE), tiene activada una línea de asistencia telefónica 900 116 117 para resolver las dudas y conflictos que habitualmente surgen en el uso de Internet y las tecnologías por parte de niños y niñas, adolescentes y sus padres y madres.

Esta línea de asesoramiento telefónico está atendida por expertos en psicología, seguridad de las tecnologías y cuestiones legales. Las llamadas se atenderán en horario de 10:00 a 20:00 horas de lunes a viernes y de 10:00 a 14:00 horas los sábados. Además, durante las 24 horas del día, los usuarios pueden remitir dudas y consultas a la dirección de correo electrónico ayuda@is4k.es.

Este servicio, de carácter confidencial y gratuito, proporciona a la menores asistencia sobre cualquiera consulta relacionada con el uso seguro y responsable de Internet y sus riesgos como pueden ser los conflictos sobre privacidad y reputación, el ciberbullying, el uso excesivo, contenidos y contactos inapropiados, comunidades peligrosas, así como cuestiones sobre protección de dispositivos, virus o fraudes, entre otros.

Junto a niños y adolescentes, también podrán hacer llamadas padres, educadores y profesionales del ámbito del menor y encontrar ayuda para hacer frente a cualquier circunstancia que pueda surgir en relación al uso de Internet.

galicia

Do mesmo xeito que todas as persoas necesitamos desenvolver as nosas competencias para manexarnos no medio físico e social, tamén precisamos ser quen de acadar plena autonomía para levar a cabo o noso proxecto vital no mundo dixital. A xestión da nosa identidade dixital, de quen somos para os demais nas redes, quen queremos ser e como percibimos e somos percibidos, require que os máis novos conten co apoio e o acompañamento que normalmente prestamos nas contornas físicas. Pero cando falamos de contornas dixitais, tan efémeras e cambiantes, familias e profesorado atopámonos con dúbidas.

No marco da Estratexia Galega de Convivencia 2015-2020 (Educonvives.gal), da man de expertos de recoñecido prestixio tanto nos seus ámbitos de coñecemento como na contorna dixital, abórdanse as dúbidas máis comúns que tanto familias como profesorado ou mesmo o alumnado ten ao respecto de cuestións que teñen que ver coa xestión da identidade dixital.

- Que é unha conexión segura?
- Como podemos exercer unha cidadanía activa e participativa en Internet?
- Que é o sexting?
- É certo que en Internet non hai fronteiras?

... así ata 50 preguntas respondidas con rigor pero cunha linguaxe clara e cercana.

Porque todos podemos e debemos ser quen de ter unha identidade dixital coa que nos sintamos a gusto.

Al igual que todas las personas necesitamos desarrollar nuestras competencias para manejarnos en el medio físico y social, también es necesario poder alcanzar plena autonomía para llevar a cabo nuestro proyecto vital en el mundo digital. La gestión de nuestra identidad digital, de quién somos para los demás en las redes, quién queremos ser y cómo percibimos y somos percibidos, requiere que los más jóvenes cuenten con el apoyo y el acompañamiento que normalmente prestamos en los entornos físicos. Pero cuando hablamos de entornos digitales, tan efímeros y cambiantes, familias y profesorado nos encontramos con dudas.

En el marco de la Estrategia Gallega de Convivencia 2015-2020 (Educonvives.gal), de la mano de expertos de reconocido prestigio tanto en sus ámbitos de conocimiento como en el entorno digital, se abordan las dudas más comunes que tanto familias como profesorado o incluso el alumnado tiene al respecto a cuestiones que tienen que ver con la gestión de la identidad digital.

- ¿Qué es una conexión segura?
- ¿Cómo podemos ejercer una ciudadanía activa y participativa en Internet?
- ¿Qué es el sexting?
- ¿Es cierto que en Internet no hay fronteras?

... así hasta 50 preguntas respondidas con rigor pero con un lenguaje claro y cercano.

Porque todos podemos y debemos ser capaces de tener una identidad digital con la que nos sintamos a gusto.

XUNTA DE GALICIA